NEBRASKA
Good Life. Great Opportunity.
DEPARTMENT OF BANKING AND FINANCE

Proposed Digital Asset Depository Nebraska Anti-Money Laundering / Countering the Financing of Terrorism and Office of Foreign Assets Control Examination Manual

Nebraska Department of Banking and Finance

Version 1.0 – October 2022

Table of Contents

1. INTRODUCTION

The Nebraska Department of Banking and Finance (or "the Department") Digital Asset Depository Institution ("DD") Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) and Office of Foreign Assets Control ("OFAC") Examination Manual (or, collectively, "DD AML & OFAC Manual") provides guidance to Department bank examiners for carrying out AML/CFT and OFAC examinations, leveraging guidance from the Federal Financial Institutions Examination Council (FFIEC)'s AML/CFT Examination Manual ("FFIEC AML Manual")[1] and federally- issued regulatory guidance on sanctions compliance.

Accordingly, this manual contains an overview of AML/CFT and sanctions compliance program requirements, AML/CFT and sanctions risks and risk management expectations, industry sound practices, and examination procedures, consistent with U.S. federal law and regulatory guidance. This DD AML & OFAC Manual supplements U.S. materials with relevant industry standards for compliance requirements specific to digital assets,[2] including the Financial Action Taskforce's 2019 *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*,[3] its subsequent *12 Month Review of Revised FATF Standards - Virtual Assets and VASPs,*[4] as well as its 2021 *Second 12 Month Review of Revised FATF Standards - Virtual Assets and VASPs*.[5] This DD AML & OFAC Manual also aligns with standards adopted by regulators in other jurisdictions[6] that have promulgated rulemaking or developed guidance related to the supervision of digital assets for regulated financial institutions, including banks or activity similar to permissible activity for DDs as appropriate.

---

[1] The DD AML & OFAC Manual leverages the 2020 version of the FFIEC AML Manual. It includes revisions made since 2020 as appropriate, including February 2021 updates (introductory section, Customer Identification Programs ("CIP"), Currency Transaction Reporting ("CTR"), and Transactions of Exempt Persons), June 2021 updates (International Transportation of Currency or Monetary Instruments Reporting, Purchase and Sale of Monetary Instruments Recordkeeping, Reports of Foreign Financial, and Special Measures), and December 2021 updates (Introduction – Customers, Charities and Nonprofit Organizations, Independent Automated Teller Machine Owners or Operators, and Politically Exposed Persons ("PEP")).

[2] Note that regulatory authorities, international organizations, and industry groups may refer to digital assets as cryptocurrency, convertible virtual currencies, virtual assets, and/or virtual currency, and these terms may be used interchangeably throughout this document. The Nebraska Financial Innovation Act refers to digital assets as controllable electronic records, i.e., "an electronic record that can be subjected to control. The term has the same meaning as digital asset and does not include electronic chattel paper, electronic documents, investment property, and transferable records under the Uniform Electronic Transactions Act." (See NRS 8-3003 (5))

[3] Financial Action Task Force (FATF), "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," (June 2019).

[4] FATF, "12 Month Review of Revised FATF Standards - Virtual Assets and VASPs" (July 2020).

[5] FATF, "Second 12 Month Review of Revised FATF Standards – Virtual Assets and VASPs" (July 2021).

[6] Refer to *Appendix A. List of Digital Assets Guidance and Supervision from Other Jurisdictions*.

Philosophical Approach to Supervision

The Nebraska Department of Banking and Finance's ("Department") mission is to protect and maintain the public confidence through fair, efficient, and experienced supervision of the state-regulated financial services industries; to assist the public in their dealings with those entities; to assist those whom we regulate in a manner which allows them to remain competitive, yet maintain their soundness in compliance with the law; to fulfill our statutory responsibilities with regard to all licensees and registrants; and to investigate violations of the laws and cooperate with other agencies in seeking a timely resolution of problems and questions. In that spirit, the state of Nebraska and the Department recognize the opportunities associated with the provision of digital asset services, and in particular, the high-skill, high-wage job opportunities associated with this innovative new industry.[7] The state of Nebraska strives to be a leader in financial innovation and acknowledges that digital asset and "fintech" services will bring Nebraska into the future, helping the state attract entrepreneurs and investment. However, the state and the Department, in enacting the Nebraska Financial Innovation Act ("NFIA"), recognize that innovative new forms of financial services raise unique safety and soundness considerations, and therefore remain committed to responsible regulation and supervision, including enforcement of Know Your Customer ("KYC") requirements, prohibitions on certain lending activities, and increased capital requirements to protect consumers. Accordingly, the NFIA, and the supervision thereof, revolves around three core guiding principles:

1. Enabling innovation and economic development in the state;

2. Providing legal certainty; and

3. Enhancing consumer protections and compliance with federal and state law.

The NFIA and the Department responsible for administering this Act require compliance with all federal and state AML/CFT, beneficial ownership, and KYC requirements. Moreover, the Department recognizes that blockchain technology and associated analytics tools enable institutions and law enforcement to trace transactions in furtherance of anti-money laundering objectives. Accordingly, the Department recognizes the role that new digital asset analytics technologies will play as part of an enhanced supervision framework (see *3.6. Digital Assets Analytics* for more information).

However, the adoption of new technologies in both banks and prudential supervision calls for insight into the means by which to leverage technology effectively and comply with existing supervisory principles with risk-based, proportionate safeguards. Careful attention must be paid toward the promotion of innovation and new products with legal compliance, consumer protection,

[7] Nebraska Legislature, "Transcript Prepared by Clerk of the Legislature Transcribers Office Banking, Commerce and Insurance Committee" (February 23, 2021).

and safeguarding the state, national, and international economy, including against the use of digital assets for illicit activity.

This balanced approach underscores supervisory trends in AML/CFT and OFAC compliance. Federal banking agencies issued a *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing* in 2018.[8] The statement explains that "[i]nnovation has the potential to augment aspects of banks' AML/CFT compliance programs, such as risk identification, transaction monitoring, and suspicious activity reporting . . . The Agencies welcome these types of innovative approaches to further efforts to protect the financial system against illicit financial activity. In addition, these types of innovative approaches can maximize utilization of banks' AML/CFT compliance resources."[9]

The DD AML/CFT & OFAC Manual generally takes a principles-based, technology-neutral approach that builds upon existing AML/CFT and sanctions standards relied upon in regulated financial institutions. Where the Department has identified additional risks posed by digital assets activity based on permissible activity for DDs, the DD AML & OFAC Manual supplements the FFIEC AML Manual's approach with additional principles, guidance, and discussion specific to the needs and risks of DDs.

This philosophical approach is consistent with federal guidance, including guidance adopted by the Office of the Comptroller of the Currency, which notes:

> First, any regulation adopted should be technology-neutral, so that products, services, and processes can evolve regardless of the changes in technology that enables them. Second, any regulation should facilitate appropriate levels of consumer protection and privacy, including features that ensure transparency and informed consent. Finally, regulations on digital activities should be principle-based, rather than prescriptive, to enable effective management of evolving risks and to reduce the potential that the regulations quickly become outdated.[10]

Based on the emergent and dynamic nature of technologies supporting DD activity, the DD AML & OFAC Manual and examination process will necessarily be responsive to market trends, best practices, and supervisory developments, both within the United States and in other jurisdictions, towards the Department's goal of promoting responsible innovation while ensuring compliance with regulation and a safe and sound operating environment, in keeping with Nebraska's vision of becoming the most trusted financial home for both people and businesses.

---

[8] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency. "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing," (December 3, 2018).

[9] *Id.*

[10] Department of Treasury, Office of the Comptroller of the Currency. "Advanced Notice of Proposed Rule-Making: National Bank and Federal Savings Association Digital Activities." (2020).

Structure of Manual

To support Department examiners and ensure compliance with state and federal banking standards, this Manual builds upon the core structure of the FFIEC AML Manual and the Wyoming Special Purpose Depository Institution AML/CFT Examination Manual. The DD AML & OFAC Manual then overlays Nebraska-specific standards in **green**, based on Nebraska-specific laws, rules, or guidance that address the unique nature of the digital assets. Otherwise, this Manual and examination process draw directly from the FFIEC AML Manual to ensure consistency with and alignment to the current supervisory examination processes for AML/CFT and OFAC compliance.

In order to effectively apply resources and ensure compliance with BSA and OFAC requirements, the manual is structured to allow examiners to tailor the AML/CFT and OFAC examination scope and procedures to the specific risk profile of the banking organization. The manual consists of the following sections:

- Introduction.
- Core Examination Overview and Procedures for Assessing the AML/CFT and OFAC Compliance Program.
- Core Examination Overview and Procedures for Regulatory Requirements and Related Topics.
- DD Risks associated with Money Laundering and Terrorist Financing
- Appendixes.

The core and expanded overview sections provide narrative guidance and background information on each topic; each overview is followed by examination procedures. The "Core Examination Overview and Procedures for Assessing the AML/CFT and OFAC Compliance Program" and the "Core Examination Overview and Procedures for Regulatory Requirements and Related Topics" (core) sections serve as a platform for the AML/CFT and OFAC examination and, for the most part, address legal and regulatory requirements of the AML/CFT and OFAC compliance program. The *2.1. Scoping and Planning*," *2.2.1. AML/CFT Risk Assessment*," and *2.2.2. OFAC Risk Assessment* sections help the examiner develop an appropriate examination plan based on the risk profile of the bank. There may be instances where a topic is covered in both the core and expanded sections (e.g., on-off ramp and virtual currency funds transfers). In such instances, the core overview and examination procedures are intended to address the BSA requirements while the expanded overview and examination procedures address the ML/TF risks of the specific activity.

In January 2021, Congress passed the AML Act of 2020, which required U.S. Department of the Treasury's Financial Crimes Enforcement Network or FinCEN (in consultation with Federal functional regulators) to promulgate AML/CFT regulations. Due to the addition of the CFT, FinCEN is generally now using the term AML/CFT instead of AML/CFT. For consistency with FinCEN and the other Federal banking agencies, the FDIC will use the term AML/CFT (which includes AML/CFT) instead of AML/CFT when referring to, issuing, or amending regulations to address the requirements of the AML Act of 2020.

OFAC Compliance

While OFAC regulations are not part of the BSA, the core sections include overview and examination procedures for examining a bank's policies, procedures, and processes for ensuring compliance with OFAC sanctions. The DD AML & OFAC Manual adds OFAC/sanctions- specific examination principles and guidance, drawing primarily from the April 2019 publication, *A Framework for OFAC Compliance Commitments* ("OFAC Framework"), "Questions on Virtual

Currency" from OFAC's Frequently Asked Questions,[11] and the October 2021 OFAC publication, *Sanctions Compliance Guidance for the Virtual Currency Industry*.[12] While certain additional internal control requirements apply, OFAC's guidance on virtual currencies states that an institution's OFAC compliance obligations remain the same regardless of whether a transaction is denominated in virtual currency or traditional fiat currency.

[11] Office of Foreign Assets Controls (OFAC), "A Framework for OFAC Compliance Commitments" (April 2019). OFAC, "OFAC FAQs: Sanctions Compliance" (August 2020).

[12] OFAC, "Sanctions Compliance Guidance for Virtual Currency Industry" (October 2021).

1.1. DD Background

On May 26, 2021, Nebraska became the second state to pass a bill authorizing the chartering of digital asset (commonly known as cryptocurrency) depositorys ("DDs").[13] LB649, also known as the Nebraska Financial Innovation Act ("NFIA"), became effective on October 1, 2021, and provides guidelines on the charter, operation, supervision, and regulation of digital asset depositories. NFIA is the "statutory framework Nebraska has chosen to encourage the creation of Nebraska Digital Asset Depositories, protect digital asset consumers, preserve confidence in Nebraska Financial Institutions, and promote FinTech innovation."[14]

NFIA allows two ways to create a DD:

(1) A business may be organized and apply for a Nebraska Digital Asset Depository Institution Charter (similar to a Bank/Financial Institution organizing and applying for its initial Nebraska Charter);[15] or
(2) A Nebraska Chartered Financial Institution, as defined by the Act, may apply for authority from the Nebraska Director of Banking and Finance ("the Director") to operate a Digital Asset Depository "Department" (an amendment to a Nebraska Bank's/Financial Institution's existing Charter).[16]

The Nebraska Department of Banking and Finance is responsible for enforcing and administering the Act, which includes the drafting of rules, regulations, and other guidance documents for the emerging industry.[17]

Permissible Activities

The NFIA specifies that a DD is authorized to provide digital asset and cryptocurrency custody services. Additionally, DDs may issue stablecoins, carry on a nonlending digital asset banking business for customers, and provide payment services upon request of a customer. Finally, though prohibited from fiat currency lending, a DD may facilitate the provision of digital asset business services resulting from the interaction of customers with centralized finance or decentralized finance platforms including, but not limited to, controllable electronic record exchange, staking, controllable electronic record lending, and controllable electronic record borrowing.[18] Examples of other facilitation activities may include trading or exchanging of digital assets as well as providing sub-custodian services. Refer to *Section 10. Asset Lending* of the DD Custody &

[13] Neb. Stat. §§ 8-3001 to 8-3031 (LB 649, 2021)

[14] The Nebraska Department of Banking and Finance Website.

[15] Neb. Stat. §8-3004 (LB649, 2021)

[16] Neb. Stat. §8-3014 (LB649, 2021)

[17] The Nebraska Department of Banking and Finance, "Digital Assets."

[18] Neb. Stat. §§ 8-3001 to 8-3031 (LB 649, 2021)

Fiduciary Manual for more information on the facilitation of asset lending transactions on behalf of custody customers.

A DD shall consult with the Director and seek any necessary approval, before engaging in a substantially new activity or line of business. The activities of a particular DD will be evaluated for their consistency with law and supervisory guidance and safety and soundness, including institution management, earnings, information technology, operational controls, and AML/CFT and OFAC compliance.

AML/CFT and OFAC Considerations around Digital Assets

Digital technology has improved the efficiency and reach of digital alternatives to cash, and accelerated usage of and trading in digital assets globally[19]. However, the U.S. Treasury Financial Crimes Enforcement Network ("FinCEN") recognizes that "[virtual currencies] may create illicit finance vulnerabilities due to the global nature, distributed structure, limited transparency, and speed of the most widely utilized virtual currency systems."[20] In a March 2022 Executive Order, the White House emphasized the need for digital assets controls (including regulation, supervision, public-private engagement) given the risks associated with illicit finance, money laundering, sanctions evasion, ransomware, terrorism, and proliferation financing, among others.[21] The Department recognizes these considerations, and therefore applies AML/CFT and OFAC inherent risk factors as part of its evaluation of digital asset activities:[22]

- Whether the new product, service, or technology promotes anonymity, obfuscates transactions, or otherwise challenges an institution's ability to identify appropriately its customers or their counterparties, or implement effective customer due diligence ("CDD"), transaction monitoring, or other AML/CFT or OFAC-related measures, including sanctions screening of counterparties involved for each transaction type;[23]

[19] White House, "United States Strategy on Countering Corruption" (December 2021).

[20] Financial Crimes Enforcement Network (FinCEN). "FIN-2019-A0003: Advisory on Illicit Activity Involving Convertible Virtual Currency." (May 9, 2019).

[21] White House, "Executive Order on Ensuring Responsible Development of Digital Assets" (March 2022).

[22] Other supervisory bodies have developed similar guidance. Note for example the Abu Dhabi Global Markets – Financial Services Regulatory Authority ("FSRA") has issued criteria for what constitutes an "Accepted Virtual Asset," which include (a) Maturity / market capitalization, (b) security (c) traceability / monitoring, (d) exchange connectivity, (e) type of Distributed Ledger (DLT), (f) innovation / efficiency, and (g) practical application/functionality. See Abu Dhabi Global Markets – Financial Services Regulatory Authority, "Guidance – Regulation of Virtual Asset Activities in ADGM" (February 24, 2020), for additional background. The U.K. Financial Conduct Authority's Joint Money Laundering Steering Group also published guidance on digital asset money laundering and terrorist financing risks, including privacy or anonymity, cross-border nature, decentralized nature, segmentation, digital nature, acceptability, immutability, convertibility, and innovation. See "22: Cryptoasset exchange providers and custodian wallet providers" (July 2020) for more information on each of these factors.

[23] Per FinCEN: "New types of anonymity-enhanced CVCs have emerged that further reduce the transparency of transactions and identities as well as obscure the source of the CVC through the incorporation of anonymizing features,

- Whether the new product, service, or technology is known to be predominantly used for criminal purposes, or substantially associated with common illicit typologies, or is otherwise associated with certain negative news indicative of AML/CFT and/or OFAC-related risk exposures;
- Whether the new product, service, or technology is susceptible to market manipulation, fraud (e.g., due to market liquidity or volatility), or operational failures posing AML/CFT or OFAC risks;[24]
- Whether the new product, service, or technology has been developed and/or used by reputable entities for legitimate reasons with legal certainty and clarity around usage; [25] or
- Whether the product has been used in other regulated environments, with appropriate, documented testing and third-party verification.

As part of its review, the Department recognizes that specific digital assets may be associated with additional unique risks. For example, a new digital asset may have privacy-enhancing features built into its source code, raising the likelihood that the digital asset may be used to obfuscate the source and/or destination of funds. Refer to *4.1. On-off Ramp Exchange and Virtual Currency Funds Transfers — Overview* for additional risk factor considerations around higher-risk and anonymity-enhancing features that digital assets may pose. Absent mitigating controls and technology solutions availability to conduct appropriate reviews for source of funds on a risk-focused approach, sanctions screening, or other requirements, these individual risk factors may drive the permissibility of such digital asset usage by DDs that the Department oversees.

As a counterbalance to the unique AML/CFT and OFAC risks posed by digital assets, digital assets are associated with unique public on-chain capabilities, i.e., provenance tracing, that can be leveraged for AML/CFT and OFAC compliance. "The blockchain ledger's immutability typically allows a historical view of a virtual currency transmission between wallet addresses, providing the opportunity for greater visibility into transaction lineage than is typically found with traditional, fiat funds transfers."[26]

For additional Department considerations around permissible activity, refer to *Section 7.1.* of the DD Custody & Fiduciary Manual.

---

such as mixing and cryptographic enhancements […]. Some CVCs appear to be designed with the express purpose of circumventing anti-money laundering/countering the financing of terrorism (AML/CFT) controls." *See* footnote 17 *supra*.

[24] Note, for example, predicate ML/TF, sanctions evasion, and other illicit activity associated with securities industry, including insider trading, market manipulation, and fraud as well as FATF's "Money Laundering and Terrorist Financing in the Securities Sector" (October 2009). Also note recent enforcement actions (example, "Financial Industry Regulatory Authority Letter of Acceptance, Waiver, and Consent, No. 2016051209102" (June 2019)) that FINRA has levied for improper AML controls around microcap securities.

[25] Monetary Authority of Singapore, "Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism" (March 2020).

[26] New York Department of Financial Services, "Guidance on Use of Blockchain Analytics" (April 2022).

1.2. Role of Government Agencies in BSA and DD Supervision

Certain government agencies play a critical role in implementing BSA regulations, developing examination guidance, ensuring compliance with the BSA, and enforcing the BSA. For DDs, these agencies include the Nebraska Department of Banking and Finance, U.S. Treasury, FinCEN, and the federal banking agencies (Federal Reserve Banks and the Board of Governors of the Federal Reserve System (Federal Reserve), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), and Office of the Comptroller of the Currency (OCC)). Internationally, there are various multilateral government bodies that support the fight against money laundering and terrorist financing.

1.2.1. Nebraska Department of Banking and Finance

The Nebraska Department of Banking and Finance is a "state agency under the direct supervision of the Governor that is comprised of two sections, Financial Institutions and Bureau of Securities, that together regulate several different financial industries."[27] Among others, the Financial Institutions section is responsible for regulating state-chartered banks, which includes DDs. Generally, NFIA requires traditional Financial Institution safeguards to apply to DDs, such as: protecting digital asset consumers (Notices, Disclosures, Due Diligence on Principals, Adequate Capital); preserving digital asset service integrity (Know Your Customer, Anti-Money Laundering, Bank Secrecy Act, Due Diligence on Principals, Adequate Capital); and promoting FinTech innovation by providing Digital Asset Depository Institutions a known FinTech business environment."[28]

The Nebraska Department of Banking and Finance is responsible for enforcing and administering NFIA, "which includes the drafting of rules, regulations, and other guidance documents for the emerging industry."[29] Under NFIA, the Director has 30 days from the time a substantially complete application is received to notify the applicant of any deficiencies; once filed, the Director sets the hearing 60 – 120 days from the filing date; finally, within 90 days of the Department receiving the hearing transcript, the "Director renders a decision on the application"[30] after conducting "careful investigation and examination,"[31] including assessing whether "the applicant has offered a complete proposal for compliance with the Nebraska Financial Innovation Act."[32] The "Director may call for reports verified under oath from a digital asset depository at any time as necessary to inform the Director of the condition of the digital asset depository. Such reports shall be available

[27] The Nebraska Department of Banking and Finance, "About NDBF."

[28] Ibid

[29] The Nebraska Department of Banking and Finance, "Digital Assets."

[30] Neb. Stat. §8-3016 (LB649, 2021)

[31] Neb. Stat. §8-3018 (LB649, 2021)

[32] Ibid

to the public."[33] Additionally, "every digital asset depository is subject to examination by the department to determine the condition and resources of a digital asset depository, the mode of managing digital asset depository affairs and conducting business, the actions of officers and directors in the investment and disposition of funds, the safety and prudence of digital asset depository management, compliance with the requirements of the Nebraska Financial Innovation Act, and such other matters as the director may require."[34] Per NFIA, "a digital asset depository shall establish and maintain programs for compliance with the federal Bank Secrecy Act, in accordance with 12 CFR 208.63, as the act and rule existed on January 1, 2021."[35] Each examination, thus, will include AML/CFT and OFAC compliance consistent with this DD AML & OFAC Manual, in addition to other traditional bank examination areas and other matters relating to digital asset capital markets activities as warranted based on the DD's risk profile. While the Department generally conducts examinations following a 12-to-18-month examination cycle, it is envisioned that during each institution's three-year *de novo* period, each DD will be examined on a twelve-month cycle, or more frequently as needed, depending on the overall risk presented by the DD. After the *de novo* period has concluded, the Director will determine whether an eighteen-month cycle may be appropriate in certain circumstances, based on the size, complexity, scope of activities, risk profile, quality of control functions, geographic diversity, and use of technology relating to a particular institution.

Each DD will also be subject to ongoing transaction monitoring requirements relating to digital assets using digital asset analytics tools.

1.2.2. U.S. Treasury

The BSA authorizes the Secretary of the Treasury to require financial institutions to establish AML programs, file certain reports, and keep certain records of transactions. Certain BSA provisions have been extended to cover not only traditional depositorys, such as banks, savings associations, and credit unions, but also nonbank financial institutions, such as money services businesses, casinos, brokers/dealers in securities, futures commission merchants, mutual funds, insurance companies, and operators of credit card systems. The U.S. Treasury also conducts and publishes National Risk Assessments ("NRAs") on Money Laundering, Terrorist Financing, and Proliferation Financing that highlight significant illicit finance threats, vulnerabilities, and risks facing the U.S., including consideration of changes to the illicit finance risk environment resulting from the increased use of digital assets. [36]

---

[33] Neb. Stat. §8-3023 (LB649, 2021)

[34] Ibid

[35] Neb. Stat. §8-3003(5) (LB649, 2021)

[36] U.S. Department of the Treasury, "National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing" (March 2022).

1.2.3. FinCEN

FinCEN, a bureau of the U.S. Treasury, is the delegated administrator of the BSA. In this capacity, FinCEN issues regulation, national priorities, and interpretive guidance, provides outreach to regulated industries, supports the examination functions performed by state and federal banking agencies, and pursues civil enforcement actions when warranted. FinCEN relies on the state and federal banking agencies to examine banks within their respective jurisdictions for compliance with the BSA. FinCEN's other significant responsibilities include providing investigative case support to law enforcement, identifying, and communicating financial crime trends and patterns, and fostering international cooperation with its counterparts worldwide. As part of this DD AML & OFAC Manual's development and ongoing supervision, the Department aligns to guidance FinCEN has set forth related to digital assets.[37] Furthermore, FinCEN releases notices of proposed rulemaking ("NPRM") – where such NPRMs are applicable to DDs, DDs will be responsible for complying with the rule if and when passed.

1.2.4. Board of Governors of the Federal Reserve System

DDs are eligible to apply to become a member bank of the Federal Reserve, as long as they have a "main-chartered office in [the] state of [Nebraska]" and subject to prudential standards relating to payment system risk and other applicable factors.[38]

1.2.5. Other Federal Banking Agencies

Other federal banking agencies are responsible for the oversight of the various banking entities operating in the United States, including foreign branch offices of U.S. banks. The federal banking agencies are charged with chartering (NCUA and OCC), insuring (FDIC and NCUA), regulating, and supervising banks.[39] In the context of DD charter application process and ongoing supervision, the Department coordinates with the Federal Reserve System and other federal banking agencies as appropriate to ensure the consistency of its supervisory approach. 12 USC 1818(s)(2) and 1786(q) require that the appropriate federal banking agency include a review of the BSA compliance program at each examination of an insured depository. The federal banking agencies may use their authority, as granted under section 8 of the FDIA or section 206

[37] These include FinCEN's "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities" (June 2021); "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 9, 2019); "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 9, 2019); and "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (March 18, 2013).

[38] Neb. Rev. Stat. §8-3005 (LB649, 2021)

[39] The Federal Reserve and FDIC may collaborate with state banking agencies on the examination, oversight, and enforcement of AML/CFT for state-chartered banks.

of the FCUA, to enforce compliance with appropriate banking rules and regulations, including compliance with the BSA.

The Department and federal banking agencies require each bank and DD[40] under their supervision to establish and maintain a BSA compliance program.[41] In accordance with the USA PATRIOT Act, FinCEN's regulations require certain financial institutions to establish an AML compliance program that guards against money laundering and terrorist financing and ensures compliance with the BSA and its implementing regulations. When the USA PATRIOT Act was passed, banks under the supervision of a federal banking agency were already required by law to establish and maintain a BSA compliance program that, among other things, requires the bank to identify and report suspicious activity promptly. For this reason, 31 CFR 1020.210 states that a bank regulated by a federal banking agency is deemed to have satisfied the AML program requirements of the USA PATRIOT Act if the bank develops and maintains a BSA compliance program that complies with the regulation of its federal functional regulator[42] governing such programs. This DD AML & OFAC Manual refers to the BSA compliance program requirements as the "AML/CFT compliance program." DDs should take reasonable and prudent steps to combat money laundering and terrorist financing and to minimize their vulnerability to the risk associated with such activities.

Some banking organizations have damaged their reputations and have been required to pay civil money penalties for failing to implement adequate controls within their organization resulting in noncompliance with the BSA. In addition, due to the AML assessment required as part of the application process, AML/CFT concerns can have an impact on the bank's strategic plan. For this reason, the federal banking agencies' and FinCEN's commitment to provide guidance that assists banks in complying with the BSA remains a high supervisory priority.

The Department and federal banking agencies work to ensure that the organizations they supervise understand the importance of having an effective AML/CFT compliance program in place.

Management must be vigilant in this area, especially as business grows and new products and services are introduced. An evaluation of the bank's AML/CFT compliance program and its compliance with the regulatory requirements of the BSA has been an integral part of the supervision process for years.[43]

As part of a strong AML/CFT compliance program, the Department and federal banking agencies seek to ensure that banks and DDs have policies, procedures, and processes to identify and report

---

[40] Neb. Rev. Stat. §8-3005(5) (LB649, 2021)

[41] Refer to 12 CFR 208.63, 12 CFR 211.5(m) and 12 CFR 211.24(j) (Federal Reserve); 12 CFR 326.8 (FDIC); 12 CFR 748.2 (NCUA); 12 CFR 21.21(OCC).

[42] Federal functional regulator means: Federal Reserve, FDIC, NCUA, OCC, Securities and Exchange Commission, or U.S. Commodity Futures Trading Commission.

[43] Refer to the FFIEC AML Manual's Appendix A ("BSA Laws and Regulations"), Appendix B ("AML/CFT Directives"), and Appendix C ("AML/CFT References") for further information and guidance.

suspicious transactions to law enforcement. The agencies' supervisory processes assess whether banks and DDs have established the appropriate policies, procedures, and processes based on their AML/CFT risk to identify and report suspicious activity and that they provide sufficient detail in reports to law enforcement agencies to make the reports useful for investigating suspicious transactions that are reported.

On July 19, 2007, the federal banking agencies issued a statement (the *Interagency Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements*) setting forth the agencies' policy for enforcing specific anti-money laundering requirements of the BSA which it subsequently updated on August 8, 2020, through the *Joint Statement on Enforcement of Bank Secrecy Act/ Anti-Money Laundering Requirements*. The purpose of this joint statement is to set forth general policy guidance, including circumstances in which an Agency will issue a mandatory cease and desist order to address noncompliance with certain Bank Secrecy Act/anti-money laundering requirements, as well formal or informal enforcement actions or other supervisory actions to address BSA-related violations or unsafe or unsound banking practices or other deficiencies.[44]

1.2.6. OFAC

OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under the President's wartime and national emergency powers, as well as under authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

OFAC requirements are separate and distinct from the BSA, but both OFAC and the BSA share a common national security goal. For this reason, many financial institutions view compliance with OFAC sanctions as related to BSA compliance obligations; supervisory examination for BSA compliance is logically connected to the examination of a financial institution's compliance with OFAC sanctions. However, given the different risks and controls associated with sanctions compliance in the digital assets space, the Department separates out its OFAC review. OFAC compliance is also in-scope for each examination. Refer to *2.4. Assessing the OFAC Compliance Program* for guidance.

[44] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, "Joint Statement On Enforcement Of Bank Secrecy Act / Anti-Money Laundering Requirements" (August 2020).

1.3. Money Laundering and Terrorist Financing

The BSA is intended to safeguard the U.S. financial system and the financial institutions that make up that system from the abuses of financial crime, including money laundering, terrorist financing, and other illicit financial transactions. Money laundering and terrorist financing are financial crimes with potentially devastating social and financial effects. From the profits of the narcotics trafficker to the assets looted from government coffers by dishonest foreign officials, criminal proceeds have the power to corrupt and ultimately destabilize communities or entire economies. Terrorist networks are able to facilitate their activities if they have financial means and access to the financial system. In both money laundering and terrorist financing, criminals can exploit loopholes and other weaknesses in the legitimate financial system to launder criminal proceeds, finance terrorism, or conduct other illegal activities, and, ultimately, hide the actual purpose of their activity.

Banking organizations must develop, implement, and maintain effective and risk-based AML programs that address the ever-changing strategies of money launderers and terrorists who attempt to gain access to the U.S. financial system. A sound AML/CFT compliance program is critical in deterring and preventing these types of activities at, or through, banks and other financial institutions. Refer to the FFIEC AML Manual's Appendix F ("Money Laundering and Terrorist Financing Red Flags") for examples of suspicious activities that may indicate money laundering or terrorist financing as well as Appendix B ("Money Laundering and Terrorist Financing Red Flags Associated with Digital Assets"), which draws upon typologies and red flags identified by FinCEN, other supervisory bodies, and industry guidance.

1.3.1. Money Laundering

Money laundering is the criminal practice of processing ill-gotten gains, or "dirty" money, through a series of transactions; in this way the funds are "cleaned" so that they appear to be proceeds from legal activities. Money laundering generally does not involve currency at every stage of the laundering process. Digital assets, given the broad array of asset types, along with the ease of asset type conversion, may be vulnerable to money laundering activities, particularly when converted to more liquid assets.[45] Although money laundering is a diverse and often complex process, it basically involves three independent steps that can occur simultaneously:

Placement. The first and most vulnerable stage of laundering money is placement. The goal is to introduce the unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement. Placement techniques include structuring deposits in amounts to evade reporting requirements or commingling deposits of legal and illegal enterprises. Examples may include: dividing large amounts of currency or digital assets into conspicuous smaller sums that are deposited directly into a bank account, depositing a refund check from a

[45] Monetary Authority of Singapore, "Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism" (March 2020).

canceled vacation package or insurance policy, or purchasing a series of monetary instruments (e.g., cashier's checks or money orders) that are then collected and deposited into accounts at another location or financial institution. Refer to Appendix G ("Structuring") in the FFIEC AML Manual for additional guidance. Relevant for digital assets, placement may occur when criminals make use of registered (with weak controls and/or supervision) and unregistered entities to transmit digital assets, including through darknet marketplace, peer-to-peer exchanges, domestic and foreign-located money service businesses ("MSBs") and other financial institutions, or CVC[46] ("convertible virtual currency") kiosks (also referred to as automated teller machines or "ATMs"). Where transactions involve the conversion to or from fiat-currency (e.g., USD or other foreign currency) to digital assets, there is an increased risk in these funds being used at the placement stage.[47]

Layering. The second stage of the money laundering process is layering, which involves moving funds around the financial system, often in a complex series of transactions to create confusion and complicate the paper trail. Examples of layering include exchanging monetary instruments for larger or smaller amounts, or wiring or transferring funds to and through numerous accounts in one or more financial institutions. Layering in the context of digital assets could involve the use of money mule accounts (derived from legitimate or stolen customer information), privacy coins, decentralized exchanges, mixers or tumblers, among others, unless legitimate uses (IT security, privacy) verified by the bank exist, especially if a customer is willing to provide transaction data or other identifying information to the bank.[48] As noted in 2020 FATF guidance, the "use of virtual assets as a way of layering is the most prominent typology […] possibly due to the ease of rapid transfer (e.g., updating public addresses and fast exchanges across borders). Professional [money laundering] networks have also appeared to start exploiting this vulnerability and use virtual assets as one of their means to launder illicit proceeds."[49] Developing controls to address these characteristics is made more difficult based in recent trends, which includes use of "[Virtual Asset Service Providers] registered or operating in jurisdictions that lack AML/CFT regulation, as well as the use of multiple VASPs (local and/or overseas)" that can further obscure the transaction trail.[50] More recently, FATF published guidance stating that there has been a sizeable increase in

[46] Per FinCEN, a CVC is a type of virtual currency that either has an equivalent value as currency, or acts as a substitute for currency, and is therefore a type of "value that substitutes for currency."

[47] Monetary Authority of Singapore, "Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism" (March 2020).

[48] Ibid

[49] FATF. "12-Month Review of The Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers." (July 2020).

[50] FATF. "12-Month Review of The Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers." (July 2020).

virtual assets collected as ransomware payments used to commit and launder the proceeds of fraud, including via unhosted[51] or privacy wallets[52].[53]

Integration. The ultimate goal of the money laundering process is integration. Once the funds are in the financial system and insulated through the layering stage, the integration stage is used to create the appearance of legality through additional transactions. These transactions further shield the criminal from a recorded connection to the funds by providing a plausible explanation for the source of the funds. Examples include the purchase and resale of real estate, investment securities, foreign trusts, or other assets. In the case of digital assets, the integration stage typically involves the exchange of virtual assets into fiat and transfer of such assets back into the traditional financial system, such as to an individual's checking account (in a process commonly referred to as "off-ramping". With broader adoption of digital assets, integration may also entail use of ill-gotten digital assets to purchase high value goods as a further store of value with merchants that directly accept digital assets[54] (e.g., non-fungible token platforms and auction houses, luxury car dealers).

1.3.2. Terrorist Financing

The motivation behind terrorist financing is ideological as opposed to profit-seeking, which is generally the motivation for most crimes associated with money laundering. Terrorism is intended to intimidate a population or to compel a government or an international organization to do or abstain from doing any specific act through the threat of violence. An effective financial infrastructure is critical to terrorist operations. Terrorist groups develop sources of funding that are relatively mobile to ensure that funds can be used to obtain material and other logistical items needed to commit terrorist acts. Thus, money laundering is often a vital component of terrorist financing.

Terrorists generally finance their activities through both unlawful and legitimate sources. Unlawful activities, such as extortion, kidnapping, and narcotics trafficking, have been found to be a major source of funding. Other observed activities include smuggling, fraud, theft, robbery, identity theft,

---

[51] An unhosted wallet, also referred to as a non-custodial, self-hosted, or non-hosted wallet, is directly controlled by the wallet owner without the requirement of an intermediary, such as an exchange. In contrast, a custodial or hosted wallet describes a wallet where a custodian (as a standalone custodial wallet service, trust company, exchange, or bank) maintains the customer's private keys and holds the customer's assets on the customer's behalf.

[52] Privacy wallets, also called mixing-enabled wallets, allow transfers where multiple people's transactions are combined into a single transfer. Privacy wallets are considered higher risk for AML and sanctions given their ability to obfuscate the origin of funds.

[53] FATF, "Second 12 Month Review of Revised FATF Standards - Virtual Assets and VASPs" (July 2021).

[54] Monetary Authority of Singapore, "Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism" (March 2020).

use of conflict diamonds,[55] and improper use of charitable or relief funds. In the last case, donors may have no knowledge that their donations have been diverted to support terrorist causes.

Other legitimate sources have also been found to provide terrorist organizations with funding; these legitimate funding sources are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership, and personal employment.

Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to those methods used by other criminals that launder funds. For example, terrorist financiers use currency smuggling, structured deposits or withdrawals from bank accounts; purchases of various types of monetary instruments; credit, debit, or prepaid cards; and funds transfers.

There is also evidence that some forms of informal banking (e.g., "hawala"[56]) have played a role in moving terrorist funds. Transactions through hawalas are difficult to detect given the lack of documentation, their size, and the nature of the transactions involved. Funding for terrorist attacks does not always require large sums of money, and the associated transactions may not be complex.

In addition to sources of terrorist financing identified above, digital assets are increasingly seen as a means through which to conduct terrorist financing, especially when coupled with social media financing campaigns. Anonymity-enhancing privacy coins (coins that are "private by default" where one cannot "turn off" the privacy features) have been implicated in terrorism financing campaigns, allowing for direct solicitation of donations as well as through placement via charitable organizations.[57] There is also preliminary evidence that terrorists and entities in comprehensively sanctioned jurisdictions have begun mining privacy coins directly and receiving 'donations' through use of supporters' computing power, as well as use of unhosted wallets to transfer digital assets in order to mask the origin of funds.[58] According to the U.S. Treasury , foreign terrorist

---

[55] Conflict diamonds originate from areas controlled by forces or factions opposed to legitimate and internationally recognized governments and are used to fund military action in opposition to those governments, or in contravention of the decisions of the United Nations Security Council.

[56] "Hawala" refers to one specific type of informal value transfer system. FinCEN describes hawala as "a method of monetary value transmission that is used in some parts of the world to conduct remittances, most often by persons who seek to legitimately send money to family members in their home country. It has also been noted that hawala, and other such systems, are possibly being used as conduits for terrorist financing or other illegal activity." For additional information and guidance on hawalas and FinCEN's report to Congress in accordance with section 359 of the USA PATRIOT Act, refer to www.fincen.gov.

[57] Department of Justice. "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns", (August 2020).

[58] CNN, "Crypto Crowdfunding Terrorists: Marketplace For Jihadist Crowdfunding Found on Dark Web" (September 2018); United Nations Security Council, "Letter dated 16 July 2020 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council" (July 2020).

groups and proliferation finance networks continue to misuse correspondent banking relationships, establish multiple front and shell companies, as well as exploit the digital economy, including through mining and trading of virtual assets, and hacking virtual asset service providers.[59]

1.4. Sanctions Evasion

Sanctions are restrictions on business and economic activity with certain countries, individuals, entities, industries, or types of activity, put in place by governments using laws and regulation. The international community uses sanctions to prevent and suppress state-sponsored terrorism and terrorist financing; change the behavior of, and apply pressure on, a target country or regime; and enforce international peace and security where diplomatic efforts have failed. International bodies (e.g., the United Nations and European Union) and governments (e.g., OFAC and the UK's Office of Financial Sanctions Implementation) typically impose three types of sanctions:

1) Comprehensive: broad restrictions in dealings, including provision and facilitation of financial services (e.g., U.S. sanctions on Iran, Cuba, North Korea, Syria, etc.);
2) Targeted: restrictions on activity that relates to specific individuals, entities, or organizations (often list-based) (e.g., arms embargoes, travel bans on individuals listed by the UK government, etc.); and
3) Export Controls: related to sanctions but focused on export and re-export of controlled goods, services, technologies (e.g., dual-use goods, U.S. origin goods, etc.).

Sanctions evasion is the act of avoiding or circumventing sanctions to engage in prohibited activity without being caught. With respect to sanctions evasion using digital assets, FinCEN notes that "while large scale sanctions evasion using convertible virtual currency (CVC) by a government is not necessarily practicable, CVC exchangers and administrators and other financial institutions may observe attempted or completed transactions tied to CVC wallets or other CVC activity associated with sanctioned and other affiliated persons." [60]

1.5. Criminal Penalties for Money Laundering, Terrorist Financing, and Violations of the BSA

Penalties for money laundering and terrorist financing can be severe. A person convicted of money laundering can face up to 20 years in prison and a fine of up to $500,000.[61] Any property involved in a transaction or traceable to the proceeds of the criminal activity, including property such as loan collateral, personal property, and, under certain conditions, entire bank accounts (even if some

[59] U.S. Department of the Treasury, "National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing" (March 2022).

[60] FinCEN, "FinCEN Provides Financial Institutions with Red Flags on Potential Russian Sanctions Evasion Attempts" (March 2022).

[61] 18 USC 1956.

of the money in the account is legitimate), may be subject to forfeiture. Pursuant to various statutes, banks and individuals may incur criminal and civil liability for violating AML and terrorist financing laws. For instance, pursuant to 18 USC 1956 and 1957, the U.S. Department of Justice may bring criminal actions for money laundering that may include criminal fines, imprisonment, and forfeiture actions.[62] In addition, banks risk losing their charters, and bank employees risk being removed and barred from banking.

Moreover, there are criminal penalties for willful violations of the BSA and its implementing regulations under 31 USC 5322 and for structuring transactions to evade BSA reporting requirements under 31 USC 5324(d). For example, a person, including a bank employee, willfully violating the BSA or its implementing regulations is subject to a criminal fine of up to $250,000 or five years in prison, or both.[63] A person who commits such a violation while violating another U.S. law, or engaging in a pattern of criminal activity, is subject to a fine of up to $500,000 or ten years in prison, or both.[64] A bank that violates certain BSA provisions, including 31 USC 5318(i) or (j), or special measures imposed under 31 USC 5318A, faces criminal money penalties up to the greater of $1 million or twice the value of the transaction.[65]

1.6. Civil Penalties for Violations of the BSA and OFAC Sanctions

Pursuant to 12 USC 1818(i) and 1786(k), and 31 USC 5321, the federal banking agencies and FinCEN, respectively, can bring civil money penalty actions for violations of the BSA. Moreover, in addition to criminal and civil money penalty actions taken against them, individuals may be removed from banking pursuant to 12 USC 1818(e)(2) for a violation of the AML laws under Title 31 of the U.S. Code, as long as the violation was not inadvertent or unintentional. All of these actions are publicly available.

The Department has the authority to impose civil monetary penalties against Nebraska institutions for violations of any state statute, rule, or order of the Director relating to financial institutions or any unsafe and unsound practice, whether willfully or as a result of negligence, incompetence, or recklessness. This power includes the ability to levy civil monetary penalties for AML/CFT and OFAC non-compliance, separate from any penalties imposed by OFAC or FinCEN.

---

[62] 18 USC 981 and 982.

[63] 31 USC 5322(a).

[64] *Id.*

[65] *Id.*

In addition, OFAC has stated that it may impose civil penalties for sanctions violations under strict liability (a U.S. person may be held civilly liable for sanctions violations even without having knowledge or reason to know it was engaging in such a violation).[66]

[66] OFAC, "Sanctions Compliance Guidance for Virtual Currency Industry" (October 2021).

2. CORE EXAMINATION OVERVIEW AND PROCEDURES FOR ASSESSING THE AML/CFT AND OFAC COMPLIANCE PROGRAM

Given the novelty of permissible activity associated with the DD charter, the Department expands upon certain federal and state standards with respect to its examinations approach. At a high level, the Department aligns to the most recent updates to the FFIEC AML Manual to evaluate compliance with AML/CFT requirements.

Recognizing that compliance with OFAC standards is critical to an effective AML/CFT and OFAC Compliance Program, the Department embeds OFAC considerations as part of its overall *2.1. Scoping and Planning* to develop an overall understanding of risks the DD faces regarding money laundering, terrorist financing, sanctions evasion, and other illicit financial activity.

This section follows with *2.2. AML/CFT Risk Assessment* and *2.3. Assessing the AML/CFT Compliance Program*, and then separately, includes a review of the DD's OFAC compliance through *2.4. Assessing the OFAC Compliance Program*.[67] Based on the overall review of the DD's AML/CFT and OFAC Compliance Program, Department examiners should formulate conclusions about the adequacy of the DD's AML/CFT and OFAC compliance program; develop an appropriate supervisory response; and communicate AML/CFT and OFAC examination findings to the DD.

2.1. Scoping and Planning

2.1.1. Scoping and Planning Introduction

Objective: *Develop an understanding of the DD's money laundering, terrorist financing (ML/TF), sanctions evasion, and other illicit financial activity risk profile. Based on the DD's risk profile, develop a risk-focused examination scope, and document the Bank Secrecy Act/anti- money laundering (AML/CFT) and OFAC examination plan.*

Examiners assess the adequacy of the DD's Bank Secrecy Act/anti-money laundering (AML/CFT) compliance program, relative to its risk profile, and the DD's compliance with BSA regulatory requirements. The scoping and planning process enables examiners to understand the money laundering, terrorist financing (ML/TF), and other illicit financial activity risk profile of the DD. The scoping and planning process also enables examiners to focus their reviews of risk management practices and compliance with BSA requirements on areas of greatest potential

[67] Sections *2.2. AML/CFT Risk Assessment* and *2.3. Assessing the AML/CFT Compliance Program* leverage the April 2020 update to the FFIEC AML Manual ("Federal and State Regulators Release Updates to AML/CFT Examination Manual" (April 15, 2020)), while the *2.4. Assessing the OFAC Compliance Program* builds upon the FFIEC AML Manual's OFAC section to capture considerations from "A Framework for OFAC Compliance Commitments" (April 2019) in addition to Nebraska-specific considerations.

ML/TF, sanctions evasion, and other illicit financial activity risks. Examiners assess whether the DD has developed and implemented adequate processes to identify, measure, monitor, and control those risks and comply with BSA regulatory requirements. Given the unique circumstances under which DDs operate, the examination process also includes assessing the DD's OFAC compliance program as a required element.

The scoping and planning process should include determining AML/CFT examination staffing needs, including technical expertise, and identifying the AML/CFT examination and testing procedures to be completed. Each section in this DD AML & OFAC Manual includes an introductory overview and accompanying examination and testing procedures, as applicable, for examiners to follow with cross-references to the FFIEC AML Manual as appropriate.

For each DD examination, the scoping and planning process should be completed before the onsite portion of the examination, although some information may not be available during this process. The scope of a AML/CFT and OFAC examination varies by DD and should be tailored primarily to the DD's risk profile. Other factors to consider in determining the examination scope may include the DD's size or complexity, and organizational structure. The request letter should also be tailored to, and correspond with, the planned examination scope.[68]

The scoping and planning process generally begins with a review of the DD's charter application (and any subsequent modifications), the DD's AML/CFT risk assessment, independent testing (audit), analyses and conclusions from previous examinations, other information available through offsite and ongoing monitoring processes, request letter items received from the DD, and any applicable information drawing from ad hoc interactions between the DD and the Department.[69] Subsections of *Scoping and Planning* provide information to help examiners understand the DD's risk profile and develop the AML/CFT and OFAC examination plan.

Many DDs rely on technology to aid in AML/CFT and OFAC compliance and, therefore, the scoping and planning process should include developing an understanding of the DD's information technology sources, systems, and processes used in the AML/CFT and OFAC compliance program. This information assists examiners in the scoping and planning process to determine what, if any, additional examiner subject matter expertise is warranted. Refer to the DD Information Security Manual for additional background.

OFAC regulations are not part of the BSA, and an OFAC review is not required during each examination cycle based on current FFIEC AML Manual standards. However, OFAC compliance programs are frequently assessed in conjunction with AML/CFT examinations. In the case of DDs, the Department recognizes unique risks associated with digital assets (including the

[68] For purposes of this DD AML Manual, a request letter also means a pre-examination request list or a first day request letter. Refer to *Appendix C: DD Request Letter Items* for more information.

[69] For purposes of this Manual, references to the terms "independent testing" and "audit" are synonymous.

pseudonymous nature of certain activity and potential for cross-border exposure) and therefore requires inclusion of OFAC compliance reviews during each examination.

Consistent with federal standards, the Nebraska Department of Banking and Finance's primary role relative to OFAC is to evaluate the sufficiency of the DD's implementation of policies, procedures, and processes for complying with OFAC-administered laws and regulations, not to identify apparent OFAC violations.[70] Accordingly, the examination review should also include a detailed review of the DD's risk profile (including products and service offerings, types of transactions offered, distribution channels, customer base, and geographies) to evaluate whether the DD has sufficient controls in place. Examiners should also review the DD's OFAC Compliance Program, OFAC risk assessment, and related independent testing to determine the appropriate scope of the review. Refer to the *2.4. Assessing the OFAC Compliance Program* section for more information.

2.1.2. Risk-Focused AML/CFT and OFAC Supervision

Objective: *Based on the DD's risk profile, determine the AML/CFT and OFAC examination activities necessary to assess the adequacy of the DD's AML/CFT and OFAC compliance program and the DD's compliance with BSA and OFAC regulatory requirements.*

The Department uses a risk-focused approach for planning and performing AML/CFT and OFAC examinations, aligning to existing federal supervisory processes including the "Joint Statement on the Risk-Focused Approach to AML/CFT Supervision."[71] Examiners should assess the adequacy of the DD's AML/CFT and OFAC compliance program, relative to its risk profile, and the DD's compliance with BSA and OFAC regulatory requirements. The extent of AML/CFT and OFAC examination activities necessary to assess the DD generally depends on the DD's risk profile and the quality of risk management processes to identify, measure, monitor, and control risks, and to report potential ML/TF, sanctions evasion, and other illicit financial activity. Given that DDs vary in size, complexity, and organizational structure, each DD has a unique risk profile, and the scope of a AML/CFT and OFAC examination varies by DD.

Given the novel nature of each DD's business model and service offerings, the Department takes a conservative approach, with risk-based supervision based on an institution's activities, earnings, compliance record and structure, and other relevant factors, as determined by the Director and required by statute or rule. In practice, this includes:

[70] OFAC determines violations of its regulations.

[71] Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), the Financial Crimes Enforcement Network (FinCEN), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC). "Joint Statement on the Risk-Focused Approach to AML/CFT Supervision." (July 2019).

- Annual, onsite examinations during the (three-year) *de novo* period;[72]
- Ad hoc meetings or calls between the DD and the Department;
- Quarterly call reports;
- Follow-up on results from examination reports, independent testing results, or other sources, as well as appropriate remedial action; and
- Regular update calls with other relevant regulators (U.S. market regulators and other state, federal, and foreign bank regulators, as appropriate).

To conduct risk-focused AML/CFT and OFAC examinations, examiners should tailor their examination plans, including examination and testing procedures, to each DD's risk profile. To understand the DD's risk profile, examiners should consider available information including, but not limited to, the following:

- The DD bank charter application, with a focus on the following components of the DD:
  - Activities and Business lines;
  - Operations (including detailed business plan);
  - Information Systems (including lists or descriptions of the primary systems and flowcharts/overviews of processes related to the products and services);
  - Management Plan (including management structure along with applicable policies and procedures);
  - Other Information (including activities and functions that will be outsourced to third-party vendors related to AML/CFT and OFAC activities); and
  - Records, Systems, and Controls.
- Examiner-in-Charge ("EIC") Scoping Memorandum relating to an DD's current activities, operations, examination history and ratings;
- The DD's internal AML/CFT and OFAC risk assessment(s), and periodic reviews and updates;
- Independent testing or audits;
- Model performance and system validation results for each AML/CFT and OFAC-specific model;
- Analyses and conclusions from previous examinations;
- Management's responses, including the current status of issues, regarding independent testing or audit results and examination findings;
- Ongoing monitoring, including call reports or other reports relating to off-balance sheet activities;
- Information received from the DD in response to the DD request letter;
- Other communications with the DD;

[72] The Department will take a risk-based approach following the *de novo* period, conducting onsite examinations annually or, potentially, every eighteen months based on the DD's size and complexity and other conditions. Further, the Department has discretion to take a risk-based approach during the *de novo* period, including conducting more frequent examinations, where the overall risk presented by the DD is elevated or where particular risk concerns are identified.

- BSA reporting available from the Financial Crimes Enforcement Network (FinCEN);
- OFAC reporting (e.g., annual blocked property reports), as well as a list of any licenses maintained with OFAC (e.g., specific licenses) and any communications/agreements entered into with OFAC (e.g., tolling agreements); and
- Resolution plan.

As explained in more detail below, examiners should review the DD's AML/CFT and OFAC risk assessments and independent testing when evaluating the DD's ability to identify, measure, monitor, and control risks. AML/CFT and OFAC risk assessments, along with independent testing that properly considers and tests all risk areas (including products, services, customers, transactions, distribution channels, and geographic locations in which the DD operates and conducts business) should be leveraged to determine the AML/CFT examination and testing procedures to be performed.[73]

This DD AML & OFAC Manual provides digital asset-specific regulatory requirements, and where possible, leverages existing federal guidance. Based on the scoping and planning, the Department examination team may identify areas where the DD bank may have exposure through areas traditionally assessed as high-risk for AML/CFT and OFAC (e.g., through cross-border funds transfers or use of omnibus accounts). In such cases, Department examiners should supplement the regulatory requirements control sections in this DD AML & OFAC Manual with the FFIEC AML Manual for those traditional, fiat-based considerations.

Department examiners should leverage the FFIEC AML Manual and corresponding examination procedures for the following sections:

- Beneficial Ownership (FFIEC AML Manual)
- Currency Transaction Reporting Exceptions (FFIEC AML Manual)
- Information Sharing[74] (FFIEC AML Manual)
- Purchase and Sale of Monetary Instruments (FFIEC AML Manual)
- Funds Transfers Recordkeeping (FFIEC AML Manual)
- Special Measures (FFIEC AML Manual)

Department examiners should also include the following DD AML & OFAC Manual control sections as part of their scoping and planning:

---

[73] As appropriate, examiners should consider aspects of these risk areas, including transaction activity (such as the number and dollar amount of cash and wire transfer activity) and distribution channels (such as mobile banking or third parties), which may impact the risks. As identified above, this review should also consider the off-ledger nature of much of DD's activities and include reviews of off-balance sheet activity.

[74] Financial institutions must query their records for data matches, including accounts maintained by the named subject during the preceding 12 months and transactions conducted within the last 6 months. See "FinCEN's 314(a) Fact Sheet" (August 25, 2020). Also see the 'Voluntary Information Sharing – Section 314(b) of the USA PATRIOT Act' section of the FFIEC Manual.

- Customer Identification Program *(Section 3.1.)*
- Customer Due Diligence (*Section 3.2.*)
- Suspicious Activity Reporting (*Section 3.3.*)
- Currency Transaction Reporting (*Section 3.4.*)
- New Products, Processes, and Technologies (*Section 3.5.*)
- Digital Asset Analytics (*Section 3.6.*)
- Virtual Currency Funds Transfers Recordkeeping (*Section 3.7.*)
- Model Risk Management (*Section 3.8.*)
- BSA Record Retention Requirements (*Section 3.9.*)

Additionally, based on the DD's risk profile, the Department examination team may also consider the following activities, regulatory requirements, and related topics as part of its scoping and planning:

- Transactions of Exempt Persons (FFIEC AML Manual)
- Reports of Foreign Financial Accounts (FFIEC AML Manual)
- Concentration Accounts (FFIEC AML Manual)
- Foreign Banking and Financial Accounts Reporting (FFIEC AML Manual)
- International Transportation of Currency or Monetary Instruments (FFIEC AML Manual)

Finally, based on the DD's active or proposed activity, the Department examination team should consider the DD AML & OFAC Manual's *4. DD Risks Associated with Money Laundering and Terrorist Financing*, as well as the FFIEC AML Manual's Appendix F – Risks Associated with Money Laundering and Terrorist Financing, as warranted, based on the DD's risk profile. The Department's examination team should address all identified activities that warrant inclusion. In-scope activities could include:

- On-Off Ramp Exchange and Virtual Currency Funds Transfers (*Section 4.1.*)
- Staking-as-a-Service (*Section 4.2.*)
- Digital Assets Escrow Services (*Section 4.3.*)
- Stablecoin Networks (*Section 4.4.*)
- Virtual Currency Automated Teller Machine Owners or Operators *(Section 4.5.)*
- Politically Exposed Persons (or "PEPs") *(Section 4.6.)*
- Charities and Nonprofit Organizations *(Section 4.7.)*
- Correspondent Accounts (Foreign) *(Section 4.8.)*
- Private Banking *(Section 4.9.)*
- Nonbank Financial Institutions *(Section 4.10.)*
- Business Entities *(Section 4.11.)*

Additionally, based on the DD's risk profile, the Department examination team may also consider the following activities, customer types, and related topics as part of its scoping and planning:

- Automated Clearing House Transactions (FFIEC AML Manual)

- Third-Party Payment Processors (FFIEC AML Manual)
- Lending Activities (FFIEC AML Manual)
- Professional Service Providers (FFIEC AML Manual)
- Funds Transfers (FFIEC AML Manual)
- Electronic Banking (FFIEC AML Manual)
- Trust and Asset Management Services (FFIEC AML Manual)
- Purchase and Sale of Monetary Instruments (FFIEC AML Manual)
- Non-deposit Investment Products (FFIEC AML Manual)
- Nonresident Aliens and Foreign Individuals (FFIEC AML Manual)

AML/CFT and OFAC Risk Assessments

The scoping and planning process is guided by examiner review of the AML/CFT and OFAC risk assessments for the DD. The information contained in the AML/CFT and OFAC risk assessments assists examiners in developing an understanding of the DD's risk profile, risk-focusing the examination scope, and assessing the adequacy of the DD's overall AML/CFT and OFAC compliance program and its compliance with BSA regulatory requirements.

The *2.2.1. AML/CFT Risk Assessment* section of this DD AML & OFAC Manual provides information and procedures for examiners in determining whether the DD has developed a risk assessment process that adequately identifies the potential ML/TF, sanctions evasion, and other illicit financial activity risks within its banking operations. If the DD has not developed a AML/CFT risk assessment, this fact should be discussed with management. Refer to *2.2.2. OFAC Risk Assessment* for additional OFAC criteria to determine whether the DD has adequately identified OFAC-related risk within its banking operations.

Independent Testing

Examiners should obtain and evaluate independent testing (audit) report(s) of the DD's AML/CFT and OFAC compliance program, including any scope and supporting workpapers. The independent testing should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties (not involved in the function being tested or other BSA or OFAC-related functions at the DD that may present a conflict of interest or lack of independence). Independent testing results should be reported directly to the board of directors, or a designated board committee composed primarily, or completely, of outside directors.

The scope and quality of independent testing may provide examiners with information regarding the DD's particular risks, how these risks are being managed and controlled, and the status of the DD's BSA and OFAC compliance. Independent testing report(s) and supporting workpapers can assist examiners in understanding audit coverage and the quality and quantity of transaction testing that was performed as part of the independent testing. This knowledge assists examiners in risk-focusing the AML/CFT and OFAC examination plan by identifying areas for greater (or lesser) review, and by identifying when additional examination and testing procedures may be necessary.

If the DD's independent testing is adequate, findings from the independent testing may be leveraged to reduce the examination areas covered and the testing necessary to assess the DD's AML/CFT and OFAC compliance program. To determine the adequacy of the DD's independent testing, examiners should determine whether the testing was independent and assessed all appropriate potential ML/TF, sanctions evasion, and other illicit financial activity risks within the DD's operations. Examiners must have access to the appropriate independent testing scope and supporting workpapers to leverage findings from the DD's independent testing. Refer to the *2.3.3. AML/CFT Independent Testing* and *2.4.4. OFAC Independent Testing* sections for more information.

BSA Reporting Available from FinCEN

FinCEN Query is the system used to access all BSA reports. AML/CFT examination planning should include an analysis of BSA reports that the DD has filed, such as Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs), and CTR exemptions, for a defined time period. SARs, CTRs, and CTR exemptions may be exported, downloaded, or obtained directly online from FinCEN Query. When requesting searches from FinCEN Query, examiners should contact the appropriate person(s) within the Department sufficiently in advance of the examination start date to obtain the requested information. When a bank has recently purchased or merged with another bank, examiners should obtain SARs, CTRs, and CTR exemptions data on the acquired bank.[75]

Downloaded information from FinCEN Query may be important to the examination, as it helps examiners:

- Identify high-volume currency customers.
- Identify the volume and characteristics of SARs filed.
- Identify frequent SAR subjects.
- Identify the volume and nature of CTRs and CTR exemptions.
- Select accounts, transactions, or BSA filings for testing, if warranted.

Consistent with federal standards, the Department does not have targeted volumes or "quotas" for SAR and CTR filings. Examiners should not criticize a DD solely because the number of SARs or CTRs filed is lower than the number of SARs or CTRs filed by "peer" DDs. However, as part of the examination, examiners should consider significant changes in the volume or nature of BSA filings and assess potential reasons for these changes. DDs should pay special attention to ensure that the cyber-specific fields of filings are completed thoroughly and accurately.

Information available through FinCEN Query is sensitive, and in some instances confidential, and may only be retrieved and used by examiners for official business. The dissemination of

[75] If a bank merges with a non-bank financial institution covered by BSA filing obligations (such as an insurance company, a money services business, digital asset trust company, or a broker-dealer), the examiner should obtain relevant filings from FinCEN Query.

information obtained through FinCEN Query is subject to specific legal requirements, restrictions, and conditions. Examiners must adhere to the "FinCEN Re-Dissemination Guidelines for Bank Secrecy Act Information" and the "FinCEN Bank Secrecy Act Information Access Security Plan" when accessing information through FinCEN Query. These documents can be obtained through each agency's FinCEN Query coordinator and should be reviewed by anyone accessing FinCEN Query.

OFAC Reporting Available from OFAC

AML/CFT & OFAC examination planning should include an analysis of OFAC reports that the DD has filed, such as initial blocked property reports, annual blocked property reports, rejected transaction reports, and on demand reports for a defined time period. The scope of such an analysis should also include any voluntary self-disclosures the DD submitted to OFAC, as well as a list of any licenses maintained with OFAC (e.g., specific licenses) and any communications/agreements entered into with OFAC (e.g., tolling agreements).

Risk-Focused Testing

Examiners perform testing to assess the adequacy of the DD's AML/CFT and OFAC compliance program, relative to its risk profile, and the DD's compliance with BSA and OFAC regulatory requirements.

Examiners also perform testing to assess the implementation of policies, procedures, and processes, and to evaluate controls, information technology sources, systems, and processes used for BSA and OFAC compliance.

Testing performed during AML/CFT and OFAC examinations should be risk-focused and can take the form of testing specific transactions, or performing analytical or other reviews. Examiners must perform some testing during each AML/CFT examination cycle. Where transaction testing typically involves reviewing specific transactions or files, analytical reviews are usually higher level without transaction or file details, such as analyzing reports. Testing may also focus on any of the regulatory requirements and may address different areas of the AML/CFT compliance program, but may not be necessary for every regulation or BSA area examined. Based on each DD's risk profile, the Department will determine areas where it conducts additional transaction testing, or can build upon existing reports (e.g., from results of the DD's independent testing) following the *de novo* period.

Under a risk-focused examination approach, the size and composition of the sample selected for testing, as well as the type of testing, should be commensurate with the DD's risk profile and the examination scope. While examiners generally test different areas in successive examinations, it may be appropriate to test the same areas in successive examinations based on previous examination findings, as well as the DD's risk profile and risk assessment, including any changes therein. Examiners should limit the extent and type of testing for smaller or less complex institutions with lower risk profiles for ML/TF, sanctions evasion, and other illicit financial activity. Where DDs have instituted new or expanded digital asset-related activity, the

Department will typically verify internal DD processes in place with sample-based transaction testing based on the risk associated with that activity. Review *4. DD Risks Associated with Money Laundering and Terrorist Financing* for more information.

Examples of DD testing may include the following:

- Full screening or sampling of virtual currency funds transfers to and from the DD's accounts for different types of digital assets that the DD offers.
- Sampling suspicious activity alerts for fiat-based and digital asset systems as appropriate, discussing (at a high level) the investigation process with staff, and reviewing the decision-making process regarding SAR filings.
- Sampling sanctions screening alerts generated from OFAC-compliance tools and controls (e.g., Internet Protocol ("IP") address and geolocation blocking, virtual private network ("VPN") monitoring, email address monitoring, etc.).
- Sampling transactions to assess compliance with Travel Rule information requirements (e.g., integration of a Travel Rule partner, use of a withdrawal and deposit questionnaire, etc.).
- Determining whether reports, such as SARs, CTRs, and blocked property reports are complete and accurate.
- Comparing filed CTRs against reportable transactions that can be identified on the DD's large cash transaction report.
- Confirming the DD has collected and verified Customer Identification Program (CIP), collected customer due diligence (CDD) data on a sample of new accounts, and reviews of customer information on a risk-focused basis (e.g., wallet addresses, source of funds).
- Determining whether the DD has collected beneficial ownership information on a sample of legal entity customers by comparing internal reports with customer files.
- Determining whether independent testing findings have been reported to the board of directors, or to a designated board committee, by reviewing the board or committee minutes.
- Determining whether internal reporting (e.g., to the Board of Directors) includes AML/CFT and OFAC-related metrics, information around new products, and other relevant factors based on the DD's risk appetite.
- Comparing staff training records with the standards outlined in the DD's training policy.

When determining the testing to perform, examiners should consider changes in the DD's business strategies, geographic locations, transaction activity, products, services, customer types, distribution channels, operations, and/or technology. Banks that have had significant changes in these areas since the previous AML/CFT examination may need more extensive testing to determine the adequacy of the AML/CFT compliance program.

Testing should be sufficient to assess the DD's adherence to, and the appropriateness of, its policies, procedures, and processes. Procedures for testing are found within the specific examination procedures sections of this DD AML & OFAC Manual, or as applicable, within the FFIEC AML Manual for traditional AML/CFT and OFAC considerations. Examiners should

document in the AML/CFT examination plan the rationale regarding the extent and type of testing to be performed. The scope of testing can be expanded to address any issues or concerns identified as part of examination activities. Examiners should also document the rationale for changes to the scope of testing.

2.1.2.1. Risk-Focused AML/CFT and OFAC Supervision Examination Procedures

Objective: *Determine the examination activities necessary to assess the adequacy of the DD's AML/CFT compliance program, relative to its risk profile, and the DD's compliance with BSA regulatory requirements. If included within the scope of the examination, determine appropriate OFAC compliance examination activities.*

Procedure	Comments
1. Obtain and review the following documents, as appropriate: • DD bank charter application and supporting materials. • Other supervisory documents maintained by the Department, including business plan changes and required regulatory filings. • Prior examination reports, supporting workpapers, management's responses to any previously identified BSA issues, and any recommendations for the next examination. • The AML/CFT and OFAC risk assessment(s), if one has been completed by the DD. If the DD has not developed a AML/CFT risk assessment or an OFAC risk assessment, examiners must develop one. Refer to the *2.2. AML/CFT and OFAC Risk Assessments* section for more information. • The DD's internal and external AML/CFT and OFAC independent testing (audit) report(s), including any scope and supporting workpapers. • Management's responses, including the current status of issues, regarding independent testing or audit results and examination findings. • Any other information available through the offsite and ongoing monitoring process or from information received from the DD in response to the request letter. This may include: o BSA reporting available from FinCEN. o OFAC reporting available from OFAC.	

○ Digital asset analytics data and reports, as well as internal files and memoranda. ○ Any other information or correspondence obtained between examinations related to the AML/CFT and OFAC compliance program, including systems and processes the DD uses to monitor and filter as well as file on currency transactions and suspicious activity, law enforcement inquiries or engagements, or higher-risk banking operations.	
2. Determine whether independent testing is adequate and may be leveraged for use in assessing the DD's AML/CFT compliance program and the DD's compliance with BSA regulatory requirements. To determine the adequacy, consider whether testing was independent and assessed all appropriate potential ML/TF, sanctions evasion, and other illicit financial activity risks within the DD's operations, and consider whether access was provided to the appropriate independent testing scope and supporting workpapers.	
3. Determine whether independent testing is adequate and may be leveraged for use in assessing the DD's OFAC compliance program and the DD's compliance with OFAC regulatory requirements. To determine the adequacy, consider whether testing was independent and assessed all appropriate OFAC risks within the DD's operations, consider whether access was provided to the appropriate independent testing scope and supporting workpapers, and verify personnel conducting independent testing were able to assess business's activity.	
4. Determine whether model performance or system validation is adequate based on the DD's complexity.	

5. Review SARs, CTRs, OFAC reports (e.g., blocked property reposts, voluntary self-disclosures, etc.,) and CTR exemption information. As appropriate, determine accounts that should be considered for further testing. On a risk basis (which may include high-risk jurisdictions or specific digital asset typologies), consider and analyze the information below for unusual patterns. • High-volume currency customers or accounts with high transaction volume or frequency for digital assets, fiat-based cross-border payments, or a combination of both, based on the DD's product offerings. • Customers who process a high volume or value with foreign jurisdictions in fiat-based or digital assets activity (or both), taking into account customer profile and expected activity (e.g., retail vs. institutional customers). • The volume and characteristics of SARs filed. • Frequent SAR subjects. • The volume and nature of CTRs and CTR exemptions. • The volume of SARs and CTRs in relation to the DD's products and services, size, asset or deposit growth, and geographic locations. • The volume and nature of OFAC reports filed. • The volume of matches to 314(a) searches • The volume of 314(b) requests and responses, if applicable to the DD. • The volume of internal referrals (i.e., manual escalations provided from each line of business, operations, or other client-facing functions). • Other digital asset-specific AML/CFT and OFAC typologies identified based on the DD's risk profile, as discussed in this Manual.	

6. Review correspondence between the DD and its regulator(s), if not already completed by the examiner-in-charge or other examination personnel. In addition, review correspondence that the DD and its regulator(s) have received from, or sent to, outside regulatory and law enforcement agencies relating to AML/CFT and OFAC compliance. Communications, particularly those received from FinCEN, may provide information relevant to the examination, such as the following: • Filing errors for SARs, CTRs, and CTR exemptions from FinCEN's BSA E-Filing System. • Civil money penalties issued by, or in process from, FinCEN or state agencies. • Civil monetary penalties issued by, or in process from, OFAC. • Law enforcement subpoenas, seizures, or "keep-open" requests. • Notification of mandatory account closures of noncooperative foreign customers holding correspondent accounts as directed by the Secretary of the Treasury or the U.S. Attorney General. • Law enforcement letters acknowledging that the DD provided highly useful information, as necessary and relevant. • Participation in law enforcement-related information exchanges, as necessary and relevant.	
7. Review the DD's information technology sources, systems, and processes used in its AML/CFT and OFAC compliance program to determine whether additional examiner subject matter expertise is warranted.	
8. Review the DD's policies, procedures, and processes for complying with OFAC-administered laws and regulations. This should include the DD's OFAC risk assessment, independent testing of its OFAC compliance program, and any correspondence between the DD and OFAC (e.g., periodic reporting of prohibited transactions and, if applicable,	

annual OFAC reports on blocked property, voluntary self-disclosures, and Cautionary or No Action Letters from OFAC). Also, review the DD's use of information technology sources, systems, and processes used in its OFAC compliance program to determine whether additional examiner subject matter expertise is warranted. For example, this may include review(s) of interdiction software and governance documentation around list management and suppression rules, to the extent the DD has in place such processes.	

2.1.3. Developing the AML/CFT and OFAC Examination Plan

Objective: *Based on the DD's risk profile, develop and document the AML/CFT and OFAC examination plan, including the AML/CFT and OFAC examination and testing procedures to be completed.*

Examiners must review a DD's AML/CFT compliance program during each examination cycle by conducting appropriate examination and testing procedures.[76] While the AML/CFT examination plan may be adjusted as a result of examination findings, an initial examination plan enables the examiner to establish the examination and testing procedures needed to assess the adequacy of the DD's AML/CFT compliance program, relative to its risk profile, and the DD's compliance with BSA regulatory requirements. Based on heightened risks around OFAC considerations, the Department captures OFAC compliance as part of each examination plan.

Examiners should develop and document an initial AML/CFT examination plan based on their review of the information highlighted in the *2.1.2. Risk-Focused AML/CFT and OFAC Supervision* section in this DD AML & OFAC Manual. As depicted below, scoping and planning should take into account the specific DD's risk profile, accounting for both traditional controls, products, and entities leveraging the FFIEC AML Manual as well as digital asset-specific considerations, as identified in this DD AML & OFAC Manual.

In addition to the minimum examination and testing procedures, the following factors should be considered when determining additional examination and testing procedures, if any, to assess the adequacy of the DD's AML/CFT and OFAC compliance program and the DD's compliance with BSA regulatory requirements:

- The DD's risk profile, size or complexity, and organizational structure.
- The quality of independent testing.
- Changes to the DD's AML/CFT or OFAC compliance officer or department.
- Expansionary activities.
- Innovations and new technologies.[77]
- Changes to state- or federal-level supervision or regulations that may impact the DD's activities.
- Other relevant factors.

Examiners should also include a review of the DD's charter application, business plan, other supervisory documents, and the EIC Scoping Memorandum to analyze new products, practices, or

[76] Section 8(s) of the Federal Deposit Insurance Act and section 206(q) of the Federal Credit Union Act require a AML/CFT compliance examination during each supervisory cycle. (12 USC 1818(s); 12 USC1786(q)).

[77] Federal Reserve, FDIC, FinCEN, NCUA, and OCC, "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing" (December 2018).

technologies that the DD has introduced or plans to introduce.

Examiners should consider which examination and testing procedures in the *2.3. Assessing the AML/CFT Compliance Program* and *2.4 Assessing the OFAC Compliance Program* sections are appropriate. AML/CFT examination and testing procedures specific to the DD's products, services, customers, transactions, and geographic locations are found in *Risks Associated with Money Laundering and Terrorist Financing* of the FFIEC AML Manual as well as *4. DD Risks Associated with Money Laundering and Terrorist Financing*. For example, if the DD offers both cross-border fiat-based funds transfers, as well as virtual currency funds transfers, these offerings should both be assessed to form an overall review of the DD's control processes for inflows and outflows of activity.

Not all of the examination and testing procedures are likely to be applicable to every DD or during every examination. Examiners should document any changes to the examination plan resulting from findings that occur after the examination has started. Note, however, that examiners should take a risk-based approach that accounts for the full set of activity under which a DD operates; where the DD conducts traditional, fiat-based activities (e.g., Fedwire or concentration accounts), the examiner should also reference the FFIEC AML Manual's corresponding section and assess whether to include in its scoping phase on a risk basis.

Examiners should determine examination staffing needs based on the scope of work in the examination plan. Consideration should be given to specific AML/CFT expertise needs based on the risk and complexity of the institution as well as information technology sources, systems, and processes. For example, based on the complexity of the activity which the DD offers (e.g., more unique forms of digital assets escrow services or advanced models), the DD may require additional specialized expertise to properly assess the DD's control processes against its risk profile.

DD Request Letter Items

Once the examiner determines the necessary examination and testing procedures to be performed, the examiner should prepare a request letter to the DD. Request letter items should be based on the DD's products, services, customers, and geographic locations and should be tailored to the examination plan areas that will be reviewed rather than submitting a comprehensive list to the DD. Additional materials may be requested as needed. Examples of request letter items are detailed in *Appendix C – DD Request Letter Items*.

2.1.3.1. Developing the AML/CFT and OFAC Examination Plan Examination Procedures

Objective: *Based on the DD's risk profile, develop and document a AML/CFT and OFAC examination plan that includes the AML/CFT and OFAC examination and testing procedures to be completed.*

Procedure	Comments
1. Based on the review of relevant examination documents, in conjunction with the review of the DD's AML/CFT and OFAC risk assessments, develop and document an initial AML/CFT and OFAC examination plan. At a minimum, the plan should address: • The risk profile of the DD, including a clear description of exposure to different types of digital assets based on the DD's proposed or current activity. • The scope and adequacy of the DD's AML/CFT and OFAC independent testing and whether the independent testing can be leveraged to assist in the assessment of the DD's AML/CFT and OFAC compliance program, including compliance with BSA and OFAC regulatory requirements. • The examination staffing needs, including any subject matter expertise (BSA and non-BSA). • The scope of the AML/CFT and OFAC examination, including the examination and testing procedures necessary to assess the adequacy of the DD's AML/CFT and OFAC compliance program, the DD's compliance with BSA and OFAC regulatory requirements, and the DD's adherence to, and the appropriateness of, its policies, procedures, and processes.	
2. Based on the review of relevant examination information and the DD's	

Procedure	Comments
risk profile, determine the examination and testing procedures to be completed. Determine the request letter items that are necessary to complete those examination and testing procedures. Examples of request letter items are detailed in *Appendix C – DD Request Letter Items*. Examiners are expected to review the request letter items provided by the DD prior to their onsite work.	

2.2. AML/CFT and OFAC Risk Assessments

As identified above, this DD AML & OFAC Manual addresses AML/CFT and OFAC Risk Assessments here to capture the potential ML/TF, sanctions evasion, and other illicit financial activity risks within the DD's banking operations.

The Department will require DDs to conduct AML/CFT and OFAC risk assessments annually, or more frequently in the event of material changes, such as the launch of a major business line or product or expansion into a new market.

2.2.1. AML/CFT Risk Assessment

Objective: *Review the DD's AML/CFT risk assessment process, and determine whether the DD has adequately identified the potential ML/TF and other illicit financial activity risks within its banking operations.*

Examiners must develop an understanding of the DD's potential ML/TF, sanctions evasion, and other illicit financial activity risks to evaluate the DD's AML/CFT compliance program. This is primarily achieved by reviewing the DD's AML/CFT risk assessment during the scoping and planning process.

This section is designed to provide standards for examiners to assess the adequacy of the DD's AML/CFT risk assessment process. For considerations around the DD's OFAC risk assessment process, refer to *2.2.2. OFAC Risk Assessment.*

AML/CFT Risk Assessment Process

To assure that AML/CFT compliance programs are reasonably designed to meet BSA regulatory requirements, DDs structure their compliance programs to be risk-based. A well-developed AML/CFT risk assessment assists the DD in identifying ML/TF and other illicit financial activity risks and in developing appropriate internal controls (i.e., policies, procedures, and processes). Understanding its risk profile enables the DD to better apply appropriate risk management processes to the AML/CFT compliance program to mitigate and manage risk and comply with BSA regulatory requirements. The AML/CFT risk assessment process also enables the DD to better identify and mitigate any gaps in controls.

The AML/CFT risk assessment should provide a comprehensive analysis of the DD's ML/TF and other illicit financial activity risks. Documenting the AML/CFT risk assessment in writing is a sound practice to effectively communicate ML/TF and other illicit financial activity risks to appropriate DD personnel. The AML/CFT risk assessment should be provided to all business lines across the DD, the board of directors, management, and appropriate staff.

The development of the AML/CFT risk assessment generally involves the identification of specific risk categories (e.g., products, services, customers, transactions, distribution channels,

and geographic locations) unique to the DD, and an analysis of the information identified to better assess the risks within these specific risk categories.

Identification of Specific Risk Categories

Generally, the first step in developing the risk assessment is to identify the DD's risk categories. Money laundering, terrorist financing, or other illicit financial activities can occur through any number of different methods or channels. A spectrum of risks may be identifiable even within the same risk category. The DD's AML/CFT risk assessment process should address the varying degrees of risk associated with its products, services, customers, transactions, geographic locations, and distribution/delivery channels, as appropriate. Improper identification and assessment of risk can have a cascading effect, creating deficiencies in multiple areas of internal controls and resulting in an overall weakened AML/CFT compliance program.

The identification of risk categories is DD-specific, and a conclusion regarding the risk categories should be based on a consideration of all pertinent information. There are no required risk categories, and the number and detail of these categories vary based on the DD's size or complexity, and organizational structure. Any single indicator does not necessarily determine the existence of lower or higher risk. However, given the potentially unique nature of a DD's activities, especially when the DD's activities place a higher importance around online activity and digital channels, the Department advises DDs to consider distribution and distribution channels as key risk areas.

The subsections within *4. DD Risks Associated with Money Laundering and Terrorist Financing* provide information and discussions on certain products, services, customers, transactions, distribution channels, and geographic locations that may present unique challenges and exposures, which DDs may need to address through specific policies, procedures, and processes.

Analysis of Specific Risk Categories

Generally, the second step in developing the AML/CFT risk assessment entails an analysis of the information obtained when identifying specific risk categories. The purpose of this analysis is to assess ML/TF and other illicit financial activity risks in order to develop appropriate internal controls to mitigate overall risk. This step may involve evaluating transaction data pertaining to the DD's activities relative to products, services, customers, and geographic locations. For example, it may be useful to quantify risk by assessing the number and dollar amount of domestic and international funds transfers, the nature of private banking customers or foreign correspondent accounts, the existence of payable through accounts, and the domestic and international geographic locations where the DD conducts or transacts business. Similarly, for off-balance sheet activity around digital assets, Department examiners should be able to quantify the number of customers and different types of digital assets the DD offers (e.g., for different types of virtual currencies that the DD on-ramps or exchanges for different virtual currencies). A detailed analysis is important, because the risks associated with the DD's activities vary, particularly in the digital asset space where different assets may present very different risks based on activity and customer identity. Additionally, the appropriate level and sophistication of the analysis varies by DD.

The following example illustrates the value of the two-step risk assessment process. The information collected by two banks in the first step reflects that each sends 100 international funds transfers per day. Further analysis by the first bank shows that approximately 90 percent of its funds transfers are recurring well-documented transactions for long-term customers.

Further analysis by the second bank shows that 90 percent of its funds transfers are nonrecurring or are processed for noncustomers. While these percentages appear to be the same, the risks may be different. This example illustrates that information collected for purposes of the bank's customer identification program and developing the customer due diligence customer risk profile is important when conducting a detailed analysis. Refer to the *Customer Identification Program*, *Customer Due Diligence*, and *Appendix J – Quantity of Risk Matrix* sections of the FFIEC AML Manual as well as *3.2. Customer Due Diligence* for more information.

Various methods and formats may be used to complete the AML/CFT risk assessment; therefore, there is no expectation for a particular method or format. DD management designs the appropriate method or format and communicates the ML/TF and other illicit financial activity risks to all appropriate parties. When the DD has established an appropriate AML/CFT risk assessment process, and has followed existing policies, procedures, and processes, examiners should not criticize the DD for individual risk or process decisions unless those decisions impact the adequacy of some aspect of the DD's AML/CFT compliance program or the DD's compliance with BSA regulatory requirements. Given the novel technology[78] and potential use cases around digital assets, this section provides high-level descriptions of inherent risk categories and related criteria for: Customers and Entities, Products and Services, Transactions, Geographic Locations, and Distribution Channels. Language included below leverages applicable guidance from the 2014 version of the FFIEC AML Manual in recognition of categories – and criteria within categories – for what constitutes a sound, risk-based control structure.

Customers and Entities. Although any type of account is potentially vulnerable to money laundering or terrorist financing, by the nature of their business, occupation, or anticipated transaction activity, certain customers and entities may pose specific risks. At this stage of the risk assessment process, it is essential that DDs exercise judgment and neither define nor treat all members of a specific category of customer as posing the same level of risk. In assessing customer risk, DDs should consider other variables, such as services sought and geographic locations. The Department considers risk assessments to be a facts-and-circumstances exercise

[78] Note existing supervisory guidance in other jurisdictions that regulate digital assets recognizes that technology and a business's operations may create additional ML/TF and other illicit activity risk. For example, the Financial Services Regulatory Authority of Ontario ("FSRA") notes: "an Authorized Person must give consideration to all business risks. For example, while an issue may be identified in relation to cyber security (e.g., when dealing with hot wallets or using cloud computing to store data – being a 'technology' risk), the FSRA expects Authorized Persons to consider these risks from all perspectives to establish whether the risk triggers other issues for consideration (including ML/TF risks, technology governance and consumer protection). An Authorized Person must then use the identified risks to develop and maintain its AML/CTF policies, procedures, systems and controls and take all reasonable steps to eliminate or manage such risks." See Abu Dhabi Global Markets – Financial Services Regulatory Authority, "Guidance – Regulation of Virtual Asset Activities in ADGM" (February 24, 2020).

that requires effective communication with potential customers and a detailed understanding of all factors. Consistent with federal guidance, the Department considers blanket risk classifications of particular industries or customers (outside of illegal activity) to be inappropriate and inconsistent with safe and sound banking practices. In the context of digital assets, a review of customers and entities may consider:

- The DD's target customer markets and segments (e.g., type of business, industry type);
- The profile and number of customers identified as higher risk or otherwise require enhanced due diligence;
- The volumes and sizes of its customers' transactions and funds or value transfers, considering the usual activities and the risk profiles of its customers and risks associated with fiat- and digital-asset-based activity;
- The volumes and size of customers' transactions for inbound and outgoing activity within the digital assets space that may pose higher potential ML/TF, and other illicit financial activity risk;
- The use of any anonymity enhancing tool such as Internet Protocol (or "IP") anonymizers that obscures one's physical location, by customers (or other counterparties involved in the transaction), which should be appropriately balanced with legitimate uses of this technology; and
- The identification of the use of mixers and tumblers, or any anonymity-enhancing technologies that obscures the identities of customers and/or their counterparties (i.e., other parties involved in a transaction), absent a justifiable IT security or privacy concern relating to a customer which has an established relationship and has passed appropriate due-diligence screening.[79]

Additionally, in July 2020, the United Kingdom's Joint Money Laundering Steering Group (or JMLSG) issued guidance that includes (but is not limited to) the following digital asset specific high-risk customer risk factors. Examiners should not consider this non-binding list prescriptive or that it indicates a *prima facie* risk, but should assess whether these concepts may warrant further inquiry based on the circumstances of the DD. These factors may include whether the customer:

- "Is involved in cryptoasset mining operations (either directly or indirectly through relationships with third parties) that take place in a high-risk jurisdiction, relate to higher-risk cryptoassets (such as privacy coins) or where its organisation gives rise to higher risk;
- Is a money transmitter who is unable to produce the required KYC information and documentation;
- Uses [virtual private network or] VPN, Tor (i.e., "The Onion Router"), encrypted, anonymous or randomly generated email or a temporary email service;
- Requests an exchange to or from cash and/or privacy coins without a legitimate use;
- Persistently avoids KYC thresholds through smaller transactions (structuring);

[79] Monetary Authority of Singapore, "Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism" (March 2020).

- Requests an exchange to or from a state-sponsored virtual currency or VASP that may be used to avoid sanctions;
- Sends or receives cryptoassets to/from peer-to-peer exchanges, or funds/withdraws from/to money without using the platform's other features; and
- Exploits technological glitches or failures to his advantage."[80]

While these risk factors may not apply, Department examiners should assess the degree to which the DD considers different customer risk factors as part of its risk assessment.

Products and Services. Certain products and services offered by DDs may pose a higher risk of money laundering or terrorist financing depending on the nature of the specific product or service offered. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. In a March 2022 Executive Order, the White House highlighted the market and national security risks when decentralized finance, peer-to-peer payment, and obscure blockchain ledgers are used without proper illicit finance controls.[81]

Additionally, in July 2020, the UK's JMLSG issued guidance that includes (but is not limited to) digital asset specific high-risk risk factors, including "the ability of users:

- To make or accept payments in money from/to unknown third parties;
- To operate more than one account with the provider [or corporate accounts separate from a natural person]; or
- To operate accounts on behalf of third parties."[82]

Additionally, activities surrounding prepaid card trading services and digital assets should also be considered as high-risk.

Transactions. Certain transaction types (both fiat and digital asset) can increase money laundering, terrorist financing, or sanctions risk because they provide opportunity for high value international funds movement (SWIFT wire transfers and direct exchange network access for international institutional customers) and pseudonymous asset movement (digital asset transactions executed with unhosted wallet addresses).

---

[80] See section 22.34 from the UK Joint Money Laundering Steering Committee Group's guidance on, "Cryptoasset exchange providers and custodian wallet providers" (July 2020). Examiners should additionally consider legitimate uses of these methods, particularly when a bank customer has an established relationship with the bank and has passed required due diligence.

[81] White House, "Executive Order on Ensuring Responsible Development of Digital Assets" (March 2022).

[82] UK Joint Money Laundering Steering Committee Group, "Cryptoasset exchange providers and custodian wallet providers" (July 2020).

Geographic Locations. Identifying geographic locations that may pose a higher risk is essential to a DD's AML/CFT compliance program. DDs should understand and evaluate the specific risks associated with doing business in, opening accounts for customers from, or facilitating transactions involving certain higher-risk geographic locations. In the context of digital assets, DDs, "should take into account publicly available information about the regulatory treatment and use of cryptoassets in particular jurisdictions to assess geographical risk."[83] The White House highlighted U.S. limitations to investigate international illicit digital assets transaction flows (e.g., ransomware) due to deficient AML/CFT regulations, supervision, and enforcement abroad.[84] However, geographic risk alone does not necessarily determine a customer's or transaction's risk level, either positively or negatively. Higher-risk geographic locations can be either international or domestic. International higher-risk geographic locations generally include:

- Countries subject to OFAC sanctions, including state sponsors of terrorism.[85] Activities conducted in, or with a substantial nexus to, these jurisdictions are presumptively prohibited.
- Countries identified as supporting international terrorism under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State.[86]
- Jurisdictions determined to be "of primary money laundering concern" by the Secretary of the Treasury, and jurisdictions subject to special measures imposed by the Secretary of the Treasury, through FinCEN, pursuant to section 311 of the USA PATRIOT Act.[87]
- Jurisdictions or countries monitored for deficiencies in their regimes to combat money laundering and terrorist financing by international entities such as FATF.
- Major money laundering countries and jurisdictions identified in the U.S. Department of State's annual International Narcotics Control Strategy Report ("INCSR"), in particular, countries that are identified as jurisdictions of primary concern.[88]
- Offshore financial centers ("OFC").[89]

[83] Ibid

[84] White House, "Executive Order on Ensuring Responsible Development of Digital Assets" (March 2022).

[85] A list of such countries, jurisdictions, and governments is available on the OFAC Web site.

[86] A list of the countries supporting international terrorism appears in the U.S. Department of State's annual Country Reports on Terrorism. These reports are available on the U.S. Department of State Web site.

[87] Notices of proposed rulemaking and final rules accompanying the determination "of primary money laundering concern," and imposition of a special measure (or measures) pursuant to section 311 of the USA PATRIOT Act are available on the FinCEN Web site.

[88] The INCSR, including the lists of high-risk money laundering countries and jurisdictions, may be accessed on the U.S. Department of State's Bureau of International Narcotics and Law Enforcement Affairs Web site.

[89] OFCs offer a variety of financial products and services. For additional information, including assessments of OFCs, refer to the International Monetary Fund's OFC page.

- Other countries identified by the DD as higher-risk because of its prior experiences or other factors (e.g., legal considerations, or allegations of official corruption).[90]
- Domestic higher-risk geographic locations may include, but are not limited to, banking offices doing business within, or having customers located within, a U.S. government-designated higher-risk geographic location. Domestic higher-risk geographic locations include:
    - High Intensity Drug Trafficking Areas ("HIDTA").[91]
    - High Intensity Financial Crime Areas ("HIFCA").[92]
- The AML/CFT laws, regulations and standards of the country or jurisdiction, including those in relation to payment service providers (or virtual assets service providers ("VASPs")).[93]
- The laws/policies of jurisdictions relating to digital assets, or the lack of official guidance relating to these assets.

Distribution Channels. Identifying the risks associated with the distribution channels customers use to access products and services, which may pose a higher risk is essential to a DD's AML/CFT compliance program. In the context of digital assets for example, "the potential risks associated with the presence of an intermediary between the cryptoasset exchange provider and the customer" may need to be considered.[94] The involvement of third parties, including intermediaries and introducing brokers, for account origination and servicing is considered an increased inherent risk factor whereby third-party introduced clients may evade controls or may be subject to less robust controls than those that would otherwise be applied by the DD. Further, non-face-to-face account origination and onboarding is typically associated with a higher risk due to the potential to evade identity verification controls.

---

[90] The Basel Anti-Money Laundering (AML) Index is an additional resource that may be useful in assisting banks with evaluating geographic locations. The Basel AML Index is a composite index that evaluates indicators from various publicly available sources such as FATF, World Bank, Transparency International and World Economic Forum.

[91] The Anti-Drug Abuse Act of 1988 and The Office of National Drug Control Policy (ONDCP) Reauthorization Act of 1998 authorized the Director of ONDCP to designate areas within the United States that exhibit serious drug trafficking problems and harmfully impact other areas of the country as HIDTAs. The HIDTA Program provides additional federal resources to those areas to help eliminate or reduce drug trafficking and its harmful consequences. A listing of these areas can be found on the White House's Office of National Drug Control Policy Web site.

[92] HIFCAs were first announced in the 1999 National Money Laundering Strategy and were conceived in the Money Laundering and Financial Crimes Strategy Act of 1998 as a means of concentrating law enforcement efforts at the federal, state, and local levels in high intensity money laundering zones. A listing of these areas can be found on the FinCEN Web site.

[93] Monetary Authority of Singapore, "Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism" (March 2020).

[94] UK Joint Money Laundering Steering Committee Group, "Cryptoasset exchange providers and custodian wallet providers" (July 2020).

Updating the Risk Assessment

Generally, risk assessments are updated (in whole or in part) to include changes in the DD's products, services, customers, transactions, distribution channels, and geographic locations and to remain an accurate reflection of the DD's ML/TF and other illicit financial activity risks. For example, the DD may need to update its AML/CFT risk assessment when new products, services, and customer types are introduced, or the DD expands through mergers and acquisitions. While there is no requirement to update the AML/CFT risk assessment on a continuous or specified periodic basis, during the de novo period the Department would expect DDs to perform annual AML/CFT and OFAC risk assessments, as their risk profile is stabilized.

For DDs, the Department exercises additional caution recognizing an effective risk assessment as the cornerstone of an effective AML/CFT compliance program. Management should update its risk assessment to identify changes in the DD's risk profile, as necessary (e.g., when new products and services are introduced, existing products and services change, higher-risk customers' open and close accounts, or the DD expands through a merger or acquisitions).

Assessing the DD's AML/CFT Risk Assessment

When evaluating the AML/CFT risk assessment, examiners should focus on whether the DD has effective processes resulting in a well-developed AML/CFT risk assessment. Examiners should not take any single indicator as determinative of the existence of a lower- or higher-risk profile for the DD. The assessment of risk factors is DD-specific, and a conclusion regarding the risk profile should be based on a consideration of all pertinent information. The DD may determine that some factors should be weighted more heavily than others. For example, the number and types of funds transfers or virtual currency funds transfers may be one factor the DD considers when assessing risk. However, to identify and weigh the risks, the DD's risk assessment process may need to consider other factors associated with those funds transfers or virtual currency funds transfers, such as whether they are international or domestic, the dollar amounts involved, and the nature of the customer relationships. Regardless of the DD's approach, sound practice would be to document the factors considered, including any weighting.

Examiners should assess whether the DD has developed a AML/CFT risk assessment that identifies its ML/TF and other illicit financial activity risks. Examiners should also assess whether the DD has considered all products, services, customers, transactions, distribution channels, and geographic locations, and whether the DD analyzed the information relative to those risk categories. For example, Department examiners may assess how the DD maintains its mapping of its products and services (including each digital asset type offered for each product and service) as well as a list of exposure by geography for each activity offered. Furthermore, examiners should assess whether the DD has developed and implemented a written data governance program for AML/CFT and OFAC/sanctions-related data that supports the risk assessment exercise.

Examiners should have a general understanding of the DD's ML/TF and other illicit financial activity risks from the examination scoping and planning process. This information should be evaluated using the two-step approach detailed in the AML/CFT Risk Assessment Process

subsection above. Examiners may also refer to *Appendix J - Quantity of Risk Matrix* of the FFIEC AML Manual when completing this evaluation. Note, however, that given the novelty of activity and the DD's customer populations, some may result in a determination that the DD has high- risk activity.

Developing a AML/CFT Compliance Program Based on the AML/CFT Risk Assessment

The DD structures its AML/CFT compliance program to address its risk profile, based on the DD's assessment of risks, as well as to comply with BSA regulatory requirements.

Specifically, the DD should develop appropriate policies, procedures, and processes to monitor and control its ML/TF and other illicit financial activity risks. For example, the DD's monitoring system to identify, research, and report suspicious activity should be risk-based to incorporate any necessary additional screening for higher-risk products, services, customers, transactions, distribution channels, and geographic locations as identified by the DD's AML/CFT risk assessment. Independent testing (audit) should review the DD's AML/CFT risk assessment, including how it is used to develop the AML/CFT compliance program. Refer to *Appendix I - Risk Assessment Link to the AML/CFT Compliance Program* of the FFIEC AML Manual for a chart depicting the expected link of the AML/CFT risk assessment to the AML/CFT compliance program. The Department should assess digital asset-specific considerations as part of these risk assessment links (e.g., through review of appropriate manual controls and automated rule coverage in its transaction monitoring and digital asset analytics tools commensurate with the risks identified in the risk assessment).

Consolidated AML/CFT Risk Assessment

Banks that choose to implement a consolidated or partially consolidated AML/CFT compliance program should assess risk within business lines and across activities and legal entities.

Consolidating ML/TF and other illicit financial activity risks for larger or more complex banking organizations may assist senior management and the board of directors in identifying, understanding, and appropriately mitigating risks within and across the banking organization. To understand ML/TF and other illicit financial activity risk exposures, the banking organization should communicate across all business lines, activities, and legal entities. Identifying a vulnerability in one aspect of the banking organization may indicate vulnerabilities elsewhere.

2.2.1.1. AML/CFT Risk Assessment Examination Procedures

Objective: *Determine the adequacy of the DD's AML/CFT risk assessment process, and determine whether the DD has adequately identified the ML/TF and other illicit financial activity risks within its banking operations.*

Procedure	Comments
1. Determine whether the DD has identified ML/TF and other illicit financial activity risks associated with the products, services, customers, transactions, distribution channels, and geographic locations unique to the DD.	
2. Determine whether the DD has analyzed and assessed the ML/TF and other illicit financial activity risks within the products, services, customers, transactions, distribution channels, and geographic locations unique to the DD. For example, this should include a mapping of the DD's products and services (including each digital asset type offered for each product and service) as well as geographic exposure for each activity.	
3. Determine whether the DD has a process for updating its AML/CFT risk assessment as necessary to reflect changes in the DD's products, services, customers, transactions, distribution channels, and geographic locations and to remain an accurate reflection of its ML/TF and other illicit financial activity risks.	
4. Determine whether the DD has appropriate processes to demonstrate a link between findings from the DD's risk assessment and its control functions, resulting in an effective, risk-based AML/CFT compliance program. Taking a risk-based approach, assess the degree to which higher risk activities identified in the risk assessment are reflected as appropriate in the DD's transaction monitoring, digital asset analytics tools, and other controls.	
5. Document and discuss with the DD any findings related to the AML/CFT risk assessment process.	

6. Determine whether the DD has developed and implemented a written data governance program for AML/CFT-related data that supports the risk assessment exercise.	

2.2.2. OFAC Risk Assessment

Objective. *Assess the DD's OFAC risk assessment to evaluate whether it is appropriate for the DD's OFAC risk, taking into consideration its products, services, customers, entities, transactions, and geographic locations*.

A fundamental element of a sound OFAC compliance program is the DD's assessment of its specific product lines, customer base, distribution channels, and nature of transactions and identification of higher- risk areas for potential OFAC sanctions risk. Per OFAC guidance from 2021, DDs should also consider customers' counterparties as a key risk area and should assess the adequacy of counterparties' compliance policies and procedures.[95] Furthermore, the Department advises DDs to consider transaction types as a key risk area, especially given the recent rise in popularity in using unhosted wallets and the ML/TF risks associated with these transactions. The initial identification of higher-risk customers for purposes of OFAC may be performed as part of the DD's CIP and CDD procedures. As OFAC sanctions can reach into virtually all areas of its operations, DDs should consider all types of transactions, products, and services when conducting their risk assessment and establishing appropriate policies, procedures, and processes. An effective risk assessment should be a composite of multiple factors (as described in more detail below), and depending upon the circumstances, certain factors may be weighed more heavily than others.

Another consideration for the risk assessment is account and transaction parties. New accounts should be compared with OFAC lists prior to being opened or shortly thereafter. However, the extent to which the DD includes account parties other than accountholders (e.g., beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories, and powers of attorney) in the initial OFAC review during the account opening process, and during subsequent database reviews of existing accounts, depends on the DD's risk profile and available technology.

Based on the DD's OFAC risk profile for each area and available technology, the DD should establish policies, procedures, and processes for reviewing transactions and transaction parties (e.g., issuing bank, payee, endorser, or jurisdiction). Currently, OFAC provides guidance on transactions parties on checks. The guidance states if a DD knows or has reason to know that a transaction party on a check is an OFAC target, the DD's processing of the transaction would expose the DD to liability, especially personally handled transactions in a higher-risk area. For example, if a DD knows or has a reason to know that a check transaction involves an OFAC-prohibited party or country, OFAC would expect timely identification and appropriate action.

In evaluating the level of risk, a DD should exercise judgment and take into account all indicators of risk. Although not an exhaustive list, examples of products, services, customers, transactions, distribution channels, and geographic locations that may carry a higher level of OFAC risk include:

[95] OFAC, "Sanctions Compliance Guidance for Virtual Currency Industry" (October 2021).

- Digital asset funds transfers into/out of the DD.
- Digital asset escrow services.
- International funds transfers.
- Nonresident alien accounts.
- Foreign customer accounts.
- Cross-border ACH transactions.
- Commercial letters of credit and other trade finance products.
- Transactional electronic banking.
- Foreign correspondent bank accounts.
- Payable through accounts.
- Concentration accounts.
- International private banking.
- Overseas branches or subsidiaries.
- Involvement of unhosted wallets in transactions, to the extent reasonably practicable.
- Involvement of stablecoins in transactions.
- Involvement of counterparties that have weak or inadequate compliance procedures and controls. [96]

In September 2021, OFAC highlighted ransomware sanctions risks and designated several cyber actors[97], thereby underscoring the importance of considering these risks in conducting OFAC risk assessments. Data from blockchain analytics providers points to outsized sanctions risks associated with ransomware payments and stablecoins (e.g., given the appeal for illicit actors to use a less volatile form of digital assets), emphasizing the need for blockchain analytics solutions—such as wallet screening and transaction monitoring—to assist DDs in complying with relevant U.S. and international sanctions.[98]

Appendix M ("Quantity of Risk Matrix — OFAC Procedures") of the FFIEC AML Manual provides guidance to examiners on assessing OFAC risks facing a DD. The risk assessment can be used to assist the examiner in determining the scope of the OFAC examination. Additional information on compliance risk is posted by OFAC on its Web site under "Frequently Asked Questions."[99]

Once the DD has identified its areas with higher OFAC risk, it should develop appropriate policies, procedures, and processes to address the associated risks. Banks may tailor these policies,

---

[96] OFAC, "Sanctions Compliance Guidance for Virtual Currency Industry" (October 2021).

[97] OFAC, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (September 2021).

[98] Elliptic, "Crypto Addresses Holding NFTs Worth $532k are Among the Latest Sanctioned by OFAC" (November 2021).

[99] This guidance is available on the OFAC Web site.

procedures, and processes to the specific nature of a business line or product, taking into account risk specific to digital assets offered (e.g., anonymity-enhancing features).

General Aspects of a Sanctions Compliance Program (SCP): Conducting a Sanctions Risk Assessment

A fundamental element of a sound SCP is the assessment of specific clients, products, services, and geographic locations in order to determine potential OFAC sanctions risk. Per OFAC guidance from 2021, "appropriately customized risk assessments should reflect a company's customer or client base, products, services, supply chain, counterparties, transactions, and geographic locations, and may also include evaluating whether counterparties and partners have adequate compliance procedures."[100] The purpose of a risk assessment is to identify inherent risks in order to inform risk-based decisions and controls. The Annex to Appendix A to 31 CFR Part 501, OFAC's Economic Sanctions Enforcement Guidelines, provides an OFAC Risk Matrix that may be used by financial institutions or other entities, such as the Department, to evaluate an institution's sanctions compliance program:

I. The organization conducts, or will conduct, an OFAC risk assessment in a manner, and with a frequency, that adequately accounts for the potential risks. Such risks could be posed by its clients and customers, products, services, supply chain, intermediaries, transactions, and geographic locations, depending on the nature of the organization. As appropriate, the risk assessment will be updated to account for the root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business.

A. In assessing its OFAC risk, organizations should leverage existing information to inform the process. In turn, the risk assessment will generally inform the extent of the due diligence efforts at various points in a relationship or in a transaction. This may include:

1. On-boarding: The organization develops a sanctions risk rating for customers, customer groups, or account relationships, as appropriate, by leveraging information provided by the customer (for example, through a Know Your Customer or Customer Due Diligence process) and independent research conducted by the organization at the initiation of the customer relationship. This information will guide the timing and scope of future due diligence efforts. Important elements to consider in determining the sanctions risk rating can be found in OFAC's risk matrices.

2. Mergers and Acquisitions (M&A): As noted above, proper risk assessments should include and encompass a variety of factors and data points for each

[100] OFAC, "Sanctions Compliance Guidance for Virtual Currency Industry" (October 2021).

organization. One of the multitude of areas organizations should include in their risk assessments—which, in recent years, appears to have presented numerous challenges with respect to OFAC sanctions—are mergers and acquisitions. Compliance functions should also be integrated into the merger, acquisition, and integration process. Whether in an advisory capacity or as a participant, the organization engages in appropriate due diligence to ensure that sanctions-related issues are identified, escalated to the relevant senior levels, addressed prior to the conclusion of any transaction, and incorporated into the organization's risk assessment process. After an M&A transaction is completed, the organization's Audit and Testing function will be critical to identifying any additional sanctions-related issues.

II. The organization has developed a methodology to identify, analyze, and address the particular risks it identifies. As appropriate, the risk assessment will be updated to account for the conduct and root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business, for example, through a testing or audit function.

2.2.2.1. OFAC Risk Assessment – Examination Procedures

Objective. *Assess the DD's OFAC risk assessment to evaluate whether it is appropriate for the DD's OFAC risk, taking into consideration its products, services, customers, entities, transactions, and geographic locations*.

Procedure	Comments
1. Determine whether the DD has identified OFAC risks associated with the products, services, customers, distribution channels, transactions, and geographic locations unique to the DD.	
2. Determine whether the DD has analyzed, and assessed the OFAC risks within the products, services, customers, distribution channels, transactions, and geographic locations unique to the DD. This may include evaluating whether counterparties and partners have adequate compliance procedures.	
3. Determine whether the DD has a formalized frequency and process for updating its OFAC risk assessment as necessary to reflect changes in the DD's products, services, customers, distribution channels, transactions, and geographic locations so that it remains an accurate reflection of its OFAC risks (including appropriate risk mitigation).	
4. Determine whether the OFAC risk assessment is updated, as appropriate, based on regulatory changes, industry trends, and other factors (e.g., ransomware activity, sanctioned crypto wallet addresses holding significant USD in NFTs, etc.).	
5. Document and discuss with the DD any findings related to the OFAC risk assessment process.	
6. Determine whether the DD has developed and implemented a written data governance program for OFAC/sanctions-related data that feeds into the risk assessment exercise.	

2.3. Assessing the AML/CFT Compliance Program

2.3.1. Assessing the AML/CFT Compliance Program

Objective: *Assess whether the DD has designed, implemented, and maintains an adequate AML/CFT compliance program that complies with BSA regulatory requirements.*

DDs must establish and maintain procedures reasonably designed to assure and monitor compliance with BSA regulatory requirements (AML/CFT compliance program).[101] The AML/CFT compliance program[102] must be written, approved by the board of directors,[103] and noted in the board minutes. To achieve the purposes of the BSA, the AML/CFT compliance program should be commensurate with the DD's potential ML/TF, sanctions evasion, and other illicit financial activity risk profile.

Refer to the *2.2.1. AML/CFT Risk Assessment* section*, 2.2.2 OFAC Risk Assessment* section, and *Appendix I - Risk Assessment Link to the AML/CFT Compliance Program* of the FFIEC AML Manual for more information.

Written policies, procedures, and processes alone are not sufficient to establish and maintain a AML/CFT compliance program; practices that correspond with the DD's written policies, procedures, and processes are needed for implementation. Importantly, policies, procedures, processes, and practices should align with the DD's unique risk profile, and be reasonably designed to assure and monitor the institution's compliance with the requirements of the BSA and its implementing regulations. Furthermore, a DD should have controls that consider recent regulatory guidance, as well as relevant industry guidance (e.g., best practices, lessons learned). The AML/CFT compliance program must provide for the following requirements (consistent with 31 CFR § 1020.210[104]):

---

[101] 12 USC 1818(s) and 12 USC 1786(q).

[102] The Federal Reserve requires Edge and agreement corporations and U.S. branches, agencies, and other offices of foreign banks supervised by the Federal Reserve to establish and maintain procedures reasonably designed to ensure and monitor compliance with the BSA and related regulations (refer to Regulation K, 12 CFR 211.5(m)(1) and 12 CFR 211.24(j)(1)). Because the BSA does not apply extraterritorially, foreign offices of domestic banks are expected to have policies, procedures, and processes in place to protect against risks of money laundering and terrorist financing (12 CFR 208.63, 12 CFR 326.8, and 12 CFR 21.21).

[103] The Federal Reserve, the FDIC, and the OCC, each require the U.S. branches, agencies, and representative offices of the foreign banks they supervise operating in the United States to develop written BSA compliance programs that are approved by their respective bank's board of directors and noted in the minutes, or that are approved by delegates acting under the express authority of their respective bank's board of directors to approve the BSA compliance programs. "Express authority" means that the head office must be aware of its U.S. AML program requirements and there must be some indication of purposeful delegation.

[104] 12 CFR 208.63, 12 CFR 211.5(m), and 12 CFR 211.24(j) (Federal Reserve); 12 CFR 326.8 (FDIC); 12 CFR 748.2 (NCUA); 12 CFR 21.21 (OCC); 31 CFR 1020.210(a)(4) (FinCEN).

- A system of internal controls to assure ongoing compliance with the BSA.
- Independent testing for AML/CFT compliance.
- A designated individual or individuals responsible for coordinating and monitoring AML/CFT compliance.
- Annual training for appropriate personnel, including a documented AML/CFT training program with annual training plan for executive officers, board members and all key personnel which may be in a position to ensure the DD's AML/CFT compliance.

In addition, the AML/CFT compliance program must include a customer identification program (CIP) with risk-based procedures that enable the DD to form a reasonable belief that it knows the true identity of its customers. A AML/CFT compliance program must also include appropriate risk-based procedures for conducting ongoing customer due diligence, including enhanced due diligence, and beneficial ownership requirements, as set forth in regulations issued by the U.S. Department of the Treasury,[105] including, but not limited to:

- understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
- conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers.

The assessment of the adequacy of the DD's AML/CFT compliance program is DD-specific, and examiners should consider all pertinent information. A review of the DD's written policies, procedures, and processes is a first step in determining the overall adequacy of the AML/CFT compliance program. The completion of examination and testing procedures is necessary to support overall conclusions regarding the AML/CFT compliance program. AML/CFT examination findings should be discussed with relevant DD management, and findings must be included in the report of examination (ROE) or supervisory correspondence.

Preliminary Evaluation

Once examiners complete the review of the DD's AML/CFT compliance program, they should develop and document a preliminary assessment of the DD's program. At this point, examiners should revisit the initial AML/CFT examination plan to determine whether additional areas of review are necessary to assess the adequacy of the DD's AML/CFT compliance program, relative to its risk profile, and the DD's compliance with BSA regulatory requirements. These adjustments to the initial examination plan could be based on information identified during the review, such as a new product or business line at the DD or independent testing report findings. Examiners should document and support any changes to the examination plan, if necessary, then proceed to the applicable examination and testing procedures. Once all relevant examination and testing

[105] 31 CFR § 1020.210(b)(5).

procedures are completed as documented in the examination plan, examiners should proceed to *2.5. Developing Conclusions and Finalizing the Examination*.

2.3.1.1. Assessing the AML/CFT Compliance Program Examination Procedures

Objective: *Determine whether the DD has designed, implemented, and maintains an adequate AML/CFT compliance program that complies with BSA regulatory requirements.*

Procedure	Comments
1. Confirm that the DD's AML/CFT compliance program is written, has been approved by the board of directors, and that the approval was noted in the board minutes.	
2. Review the AML/CFT compliance program and determine whether it is tailored to the DD's ML/TF and other illicit financial activity risk profile. Determine whether the DD's compliance program contains the following requirements: • A system of internal controls to assure ongoing compliance, as well as consideration of recent regulatory guidance and industry guidance applicable to the DD. • Independent testing for compliance to be conducted by DD personnel or an outside party. • Designation of a qualified individual or individuals responsible for coordinating and monitoring day-to-day compliance (BSA compliance officer). • Training for appropriate personnel.	
3. Determine whether the DD's CIP, risk-based CDD (including enhanced due diligence, "EDD"), and beneficial ownership procedures are included as part of the AML/CFT compliance program.	
4. Determine whether the initial AML/CFT examination plan should be adjusted based on new information identified during the examination. Document and support any changes made.	

2.3.2. AML/CFT Internal Controls

Objective: *Assess the DD's system of internal controls to assure ongoing compliance with BSA regulatory requirements.*

The board of directors, acting through senior management, is ultimately responsible for ensuring that the DD maintains a system of internal controls to assure ongoing compliance with BSA regulatory requirements.[106] Internal controls are the DD's policies, procedures, and processes designed to mitigate and manage potential ML/TF, sanctions evasion, and other illicit financial activity risks and to achieve compliance with BSA regulatory requirements. The board of directors plays an important role in establishing and maintaining an appropriate culture that places a priority on compliance, and a structure that provides oversight and holds senior management accountable for implementing the DD's AML/CFT internal controls. Per DD rules, the Department sets board responsibilities, including, but not limited to:

- Review and approval of the DD's documented AML/CFT Compliance Policy;
- Review and approval of the DD's annual AML/CFT risk assessments;
- Approval of any new products and services prior to launch, including an assessment of any material risks and means through which transaction monitoring and sanctions screening will be conducted; and
- Development and maintenance of clear risk appetite standards with periodic reporting of AML/CFT-related key risk indicators ("KRIs"), key performance indicators ("KPIs"), status of any open corrective issues, and any evolving regulatory issues or industry trends.
- Periodic review of key-vendor and third-party due diligence.

The system of internal controls, including the level and type, should be commensurate with the DD's size or complexity, and organizational structure. Large or more complex DDs may implement specific departmental internal controls for AML/CFT compliance. Departmental internal controls typically address risks and compliance requirements unique to a particular line of business or department and are part of a comprehensive, DD-wide AML/CFT compliance program.

Examiners should determine whether the DD's internal controls are designed to assure ongoing compliance with BSA regulatory requirements and whether internal controls take into consideration applicable recent regulatory guidance and industry guidance. When reviewing internal controls, examiners should consider whether internal controls:

- Incorporate the DD's AML/CFT risk assessment and the identification of potential ML/TF, sanctions evasion, and other illicit financial activity risks, along with any changes in those risks.

[106] 12 CFR 208.63(c)(1), (Federal Reserve); 12 CFR 326.8(c)(1) (FDIC); 12 CFR 748.2(c)(1) (NCUA); 12 CFR21.21(d)(1) (OCC); 31 CFR 1020.210 (FinCEN).

- Provide for program continuity despite changes in operations, management, or employee composition or structure.
- Facilitate oversight of information technology sources, systems, and processes that support AML/CFT compliance.
- Provide for timely updates in response to changes in regulations and the rapidly evolving digital assets landscape (i.e., the "continued trend of rapid technological progress in the VASP sector"[107]).
- Incorporate dual controls and the segregation of duties to the extent possible. For example, employees who complete the reporting forms (such as suspicious activity reports (SARs), currency transaction reports (CTRs), and CTR exemptions) generally should not also be responsible for the decision to file the reports or grant the exemptions.
- Include mechanisms to identify and inform the board of directors, or a committee thereof, and senior management of BSA compliance initiatives, including the annual risk assessment and any new products, processes, or technologies underway; identified compliance deficiencies and corrective action taken, as well as the AML/CFT-related KPIs or KRIs relevant to the DD's risk appetite; and notify the board of directors of SARs filed.
- Incorporate management information ("MI") reporting of abovementioned AML/CFT KPIs and KRIs, as well as transaction and trend analyses as they pertain to BSA compliance.
- Include a written data governance program for AML/CFT-related MIS that feeds into various reports.
- Include a formal issues management process with written policies and procedures defining how to identify, escalate (or report), and remediate AML/CFT compliance-related issues.
- Identify the qualifications required of BSA compliance personnel (including senior management) and develop/implement resourcing and succession planning documentation to ensure there is sufficient BSA knowledge and resources amongst compliance staff.
- Identify and establish specific BSA compliance responsibilities for DD personnel and provide oversight for execution of those responsibilities, as appropriate.
- Include controls specific to transaction monitoring (e.g., blockchain analytics, behavioral analytics, and digital asset coverage), identification of hosted vs. unhosted wallets (to the extent this is operationally feasible and required by regulation), CIP, CDD, and EDD by customer type, and recordkeeping requirements under the Travel Rule.

This list is not all-inclusive and should be tailored to reflect the DD's risk profile. More information concerning individual regulatory requirements and specific risk areas is in the *Assessing Compliance with BSA Regulatory Requirements* and *Appendix B: Money Laundering and Terrorist Financing Red Flags Associated with Digital Assets* and *Risks Associated with*

[107] FATF, "Second 12 Month Review of Revised FATF Standards - Virtual Assets and VASPs" (July 2021).

Money Laundering and Terrorist Financing in the FFIEC AML Manual.

Examiners should determine whether the DD's system of internal controls is designed to mitigate and manage the ML/TF, and other illicit financial activity risks, and comply with BSA regulatory requirements. Examiners should assess the adequacy of internal controls based on the factors listed above.

2.3.2.1. AML/CFT Internal Controls Examination Procedures

Objective: *Determine whether the DD has implemented a system of internal controls that assures ongoing compliance with BSA regulatory requirements.*

Procedure	Comments
1. Determine whether the DD's system of internal controls (i.e., policies, procedures, and processes) is designed to: • Mitigate and manage potential ML/TF and other illicit financial activity risks, and • Assure ongoing compliance with BSA regulatory requirements and consider applicable recent regulatory guidance and industry guidance.	
2. Determine whether the internal controls: • Incorporate the DD's AML/CFT risk assessment and the identification of potential ML/TF and other illicit financial activity risks, along with any changes in those risks. • Provide for program continuity despite changes in operations, management, or employee composition or structure. • Facilitate oversight of information technology sources, systems, and processes that support AML/CFT compliance. • Provide for timely updates to implement changes in regulations, as well as to account for the rapidly evolving digital assets landscape (e.g., industry developments and practices). • Incorporate dual controls and the segregation of duties to the extent possible. • Include mechanisms to identify and escalate BSA compliance issues to management and the board of directors, or a committee thereof, as appropriate.	

Procedure	Comments
• Inform the board of directors, or a committee thereof, and senior management of compliance initiatives; including the annual risk assessment and any new products, processes, or technologies; identified compliance deficiencies, and corrective action taken, as well as the AML/CFT-related KPIs or KRIs relevant to the DD's risk appetite; and notification to the board of directors of SARs filed. • Include regular management information ("MI") reporting of AML/CFT KPIs and KRIs, as well as transaction and trend analyses as they pertain to AML/CFT compliance. • Include a written data governance program for AML/CFT-related MIS that feeds into various reports. • Include a formal issues management process with written policies and procedures defining how to identify, escalate (or report), and remediate sanctions compliance-related issues. • Identify the qualifications required of BSA compliance personnel (including senior management) and whether resourcing and succession planning documentation has been developed and implemented to ensure there is sufficient BSA knowledge and resources amongst compliance staff. • Identify and establish specific BSA compliance responsibilities for DD personnel and provide oversight for execution of those responsibilities, as appropriate. • Include controls specific to transaction monitoring (e.g., blockchain analytics, behavioral analytics, and digital asset coverage), identification of hosted vs.	

Procedure	Comments
unhosted wallets (to the extent this is operationally feasible and required by regulation), CIP, CDD, and EDD by customer type, and recordkeeping requirements under the Travel Rule. *Refer to 3.1., 3.2., 3.6. and 3.7. for additional digital asset-specific considerations for AML/CFT internal controls.*	

2.3.3. AML/CFT Independent Testing

Objective: *Assess the adequacy of the DD's independent testing program*.

The purpose of independent testing (audit) is to assess the DD's compliance with BSA regulatory requirements, relative to its risk profile, and assess the overall adequacy of the AML/CFT compliance program. Independent testing should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties.[108]

DDs that do not employ outside auditors or consultants or do not have internal audit departments may comply with this requirement by using qualified DD staff who are not involved in the function being tested. DDs engaging outside auditors or consultants should ensure that the persons conducting the AML/CFT independent testing are not involved in other BSA-related functions at the DD that may present a conflict of interest or lack of independence, such as training or developing policies and procedures. Regardless of who performs the independent testing, the party conducting the AML/CFT independent testing should report directly to the board of directors or to a designated board committee comprised primarily, or completely, of outside directors. DDs with a community focus, less complex operations, and lower-risk profiles for ML/TF and other illicit financial activities may consider utilizing a shared resource as part of a collaborative arrangement to conduct independent testing.[109]

There is no federal regulatory requirement establishing AML/CFT independent testing frequency. Independent testing, including the frequency, should be commensurate with the risk-profile of the DD and the DD's overall risk management strategy. The DD may conduct independent testing over periodic intervals (for example, every 12–18 months) and/or when there are significant changes in the DD's risk profile, systems, compliance staff, or processes. More frequent independent testing may be appropriate when errors or deficiencies in some aspect of the AML/CFT compliance program have been identified or to verify or validate mitigating or remedial actions. However, it is strongly encouraged that DDs conduct independent testing **annually** with personnel with a skillset appropriately tailored to evaluate the unique risks identified based on the DD's risk profile.

Independent testing of specific BSA requirements should be risk-based and evaluate the quality of risk management related to potential ML/TF and other illicit financial activity risks for significant operations across the organization. Risk-based independent testing focuses on the DD's risk assessment to tailor independent testing to the areas identified as being of greatest risk and concern, as identified internally through the Board's risk appetite, evolving regulatory concerns or industry trends, or based on other criteria as defined by the DD. Risk-based independent testing programs

---

[108] 12 CFR 208.63(c)(2) (Federal Reserve); 12 CFR 326.8(c)(2) (FDIC); 12 CFR 748.2(c)2) (NCUA); 12 CFR 21.21(d)(2) (OCC)

[109] For detailed information on collaborative arrangements see "Interagency Statement on Sharing Bank Secrecy Act Resources," issued by Federal Reserve, FDIC, FinCEN, NCUA, and OCC (October 3, 2018).

vary depending on the DD's size or complexity, organizational structure, scope of activities, risk profile, quality of control functions, geographic diversity, and use of technology. Risk-based independent testing should include evaluating pertinent internal controls and information technology sources, systems, and processes used to support the AML/CFT compliance program, including those specific to DDs such as digital asset analytics, virtual currency funds transfers recordkeeping and other DD-specific controls depending on the DD's risk profile. Consideration should also be given to the expansion into new product lines, services, customer types, and geographic locations through organic growth or merger activity.

The independent testing should evaluate the overall adequacy of the DD's AML/CFT compliance program and the DD's compliance with BSA regulatory requirements. This evaluation helps inform the board of directors and senior management of weakness, or areas in need of enhancements or stronger controls. Typically, this evaluation includes an explicit statement in the report(s) about the DD's overall compliance with BSA regulatory requirements. At a minimum, the independent testing should contain sufficient information for the reviewer (e.g., board of directors, senior management, BSA compliance officer, review auditor, or an examiner) to reach a conclusion about the overall adequacy of the AML/CFT compliance program.

To contain sufficient information to reach this conclusion, independent testing of the AML/CFT compliance program and BSA regulatory requirements may include a risk-based review of whether:

- The DD's AML/CFT risk assessment aligns with the DD's risk profile (products, services, customers, transactions, delivery channels, and geographic locations).
- The DD's policies, procedures, and processes for BSA compliance align with the DD's risk profile.
- The DD adheres to its policies, procedures, and processes for BSA compliance.
- The DD complies with BSA recordkeeping and reporting requirements (e.g., customer information program (CIP) (including electronic verification), customer due diligence (CDD) (including enhanced due diligence), beneficial ownership, appropriate source of funds reviews on a risk-focused basis, suspicious activity reports (SARs), currency transaction reports (CTRs) and CTR exemptions, and information sharing requests).
- The DD's overall process for identifying and reporting suspicious activity is adequate. This review may include evaluating filed or prepared SARs to determine their accuracy, timeliness, completeness, and conformance to the DD's policies, procedures, and processes. It may also review alerts generated and SARs filed to assess that the DD has a full picture of the customer's activity to identify unusual activity.
- The DD's information technology sources, systems, and processes used to support the AML/CFT compliance program are complete and accurate. These may include reports or automated programs used to: identify large currency transactions, aggregate daily currency transactions, record monetary instrument sales and funds transfer transactions, and provide analytical and trend reports.
- The DD's use of digital asset analytics to support AML/CFT compliance align to the

DD's risk profile. This could include a review of how the DD integrates digital asset analytics into its overall AML/CFT Compliance Program with appropriate model risk management in place.

- The DD's use of artificial intelligence ("AI") tools and/or "big data" (in addition to advanced analytics), if applicable.
- Training is provided for appropriate personnel, tailored to specific functions and positions, and includes supporting documentation.
- Management took appropriate and timely action to address any violations and other deficiencies noted in previous independent testing and regulatory examinations, including progress in addressing outstanding supervisory enforcement actions, if applicable.

Auditors should document the independent testing scope, procedures performed, transaction testing completed, and any findings. All independent testing documentation and supporting workpapers should be available for examiner review. Violations; exceptions to DD policies, procedures, or processes; or other deficiencies noted during the independent testing should be documented and reported to the board of directors or a designated board committee in a timely manner. The board of directors, or a designated board committee, and appropriate staff should track deficiencies and document progress implementing corrective actions.

Examiners should review relevant documents such as the auditor's report(s), scope, and supporting workpapers, as needed. Examiners should determine whether there is an explicit statement in the report(s) about the DD's overall compliance with BSA regulatory requirements or, at a minimum, sufficient information to reach a conclusion about the overall adequacy of the AML/CFT compliance program. Examiners should determine whether the testing was conducted in an independent manner. Examiners may also evaluate, as applicable, the subject matter expertise, qualifications and independence of the person or persons performing the independent testing. Examiners should determine whether the independent testing sufficiently covers potential ML/TF and other illicit financial activity risks within the DD's operations and whether the frequency is commensurate with the DD's risk profile. As appropriate, this could include a review to determine whether compliance testing as a second line of defense is in place depending on the risk, size, and complexity of the DD. Examiners should also review whether violations; exceptions to policies, procedures, or processes; or other deficiencies are reported to the board of directors or a designated board committee in a timely manner, whether they are tracked, and whether corrective actions are documented.

2.3.3.1. AML/CFT Independent Testing Examination Procedures

Objective: *Determine whether the DD has designed, implemented, and maintains an adequate AML/CFT independent testing program for compliance with BSA regulatory requirements.*

Procedure	Comments
1. Determine whether the AML/CFT independent testing (audit) is independent (i.e., performed by a person or persons not involved with the function being tested or other BSA-related functions at the DD that may present a conflict of interest or lack of independence).	
2. Determine whether in addition to independent testing the DD also has a compliance monitoring and testing function that performs their own reviews of key AML/CFT controls; if yes, evaluate the scope and adequacy of these reviews.	
3. Determine whether independent testing addresses the overall adequacy of the AML/CFT compliance program, including policies, procedures, and processes. Typically, the report includes an explicit statement about the DD's overall compliance with BSA regulatory requirements. At a minimum, the independent testing should contain sufficient information for the reviewer to reach a conclusion about the overall adequacy of the AML/CFT compliance program.	
4. Through a review of board minutes or other board of directors' materials, determine whether persons conducting the independent testing reported directly to the board of directors or to a designated board committee comprised primarily, or completely, of outside directors. Determine whether independent testing results were provided to the board of directors and senior management.	

Procedure	Comments
5. Review independent testing reports, scope, and supporting workpapers to determine whether they are comprehensive, accurate, adequate, and timely, relative to the DD's risk profile. Examiners may also evaluate, as applicable, the subject matter expertise, qualifications, and independence of the person or persons performing the independent testing.[110] Although there are no specific regulatory requirements for the development of an independent test, consider whether the independent testing includes, as applicable, an evaluation of: • The AML/CFT risk assessment. • The relevant changes in DD activities since the last independent test. • The policies, procedures, and processes governing the AML/CFT compliance program and other BSA regulatory requirements, and personnel's adherence to those policies, procedures, and processes. • The DD's adherence to BSA reporting and recordkeeping requirements. • The DD's information technology sources, systems, and processes used to support the AML/CFT compliance program and whether they are complete and accurate. These may include reports or automated programs used to: identify large currency transactions, aggregate daily currency transactions, record monetary instrument sales and funds transfer transactions, and provide analytical and trend reports. • Training for appropriate personnel and whether it is tailored to specific	

[110] For more information, see e.g., OCC Safety and Soundness Standards, 12 CFR Part 30 App. D, II. L.

Procedure	Comments
functions and positions and includes supporting documentation. • Management's actions to appropriately and timely address any violations and other deficiencies noted in previous independent testing and regulatory examinations, including progress in addressing outstanding supervisory enforcement actions, if applicable.	
6. Determine whether independent testing includes, as applicable, an evaluation of suspicious activity monitoring systems and the system's ability to identify potentially suspicious activity. Although there are no specific regulatory requirements for the development of an independent test, consider whether the independent testing includes, as applicable, an evaluation of: • The system's methodology for monitoring transactions and accounts for potentially suspicious activity. • The system's ability to generate monitoring reports. • Filtering criteria, as appropriate, to determine whether they are reasonable, tailored to the DD's risk profile, and include higher-risk products, services, customers, and geographic locations. • Policies, procedures, and processes for suspicious activity monitoring systems. Refer to *3.8. Model Risk Management* for additional considerations for any AML/CFT and OFAC models the DD intends to use or has in production.	
7. Determine whether the independent testing includes a review and evaluation of the overall suspicious activity monitoring and reporting process. Although there are no specific regulatory requirements for the development of an independent test,	

Procedure	Comments
consider whether the independent testing includes, as applicable, an evaluation of: • The identification or alert process. • The management of alerts, research, SAR decision making, SAR completion and filing, and monitoring of continuous activity. • Policies, procedures, and processes for referring potentially suspicious activity from all operational areas and business lines (such as, trust services, private banking, foreign correspondent banking) to the personnel or department responsible for evaluating potentially suspicious activity.	
8. Determine whether the independent testing performed was adequate, relative to the DD's risk profile.	

2.3.4. BSA Compliance Officer

Objective: *Confirm that the DD's board of directors has designated a qualified individual or individuals (BSA compliance officer) responsible for coordinating and monitoring day-to-day compliance with BSA regulatory requirements. Assess whether the BSA compliance officer has the appropriate authority, independence, access to resources, and competence to effectively execute all duties.*

The DD's board of directors must designate a qualified individual or individuals to serve as the BSA compliance officer.[111] The BSA compliance officer is responsible for coordinating and monitoring day-to-day AML/CFT compliance. The BSA compliance officer is also charged with managing all aspects of the AML/CFT compliance program, including managing the DD's compliance with BSA regulatory requirements. The board of directors is ultimately responsible for the DD's AML/CFT compliance and should provide oversight for senior management and the BSA compliance officer in the implementation of the DD's board-approved AML/CFT compliance program.[112]

The act by the DD's board of directors of appointing a BSA compliance officer is not, by itself, sufficient to meet the regulatory requirement to establish and maintain a AML/CFT compliance program reasonably designed to assure and monitor compliance with the BSA. The board of directors is responsible for ensuring that the BSA compliance officer has appropriate authority, independence, and access to resources to administer an adequate AML/CFT compliance program based on the DD's ML/TF and other illicit financial activity risk profile. The BSA compliance officer should regularly report the status of ongoing compliance with the BSA to the board of directors and senior management so that they can make informed decisions about existing risk exposure and the overall AML/CFT compliance program. Reporting to the board of directors or a designated board committee about the status of ongoing compliance should include pertinent BSA-related information, including the required notification of suspicious activity report (SAR) filings.

The BSA compliance officer is responsible for carrying out the board's direction, including the implementation of the DD's AML/CFT policies, procedures, and processes. The BSA compliance officer may delegate AML/CFT duties to staff, but the officer is responsible for overseeing the day-to-day AML/CFT compliance program.

The BSA compliance officer should be competent, as demonstrated by knowledge of the BSA and related regulations, implementation of the DD's AML/CFT compliance program, and understanding of the DD's risk profile associated with its activities, including appropriate digital asset background and expertise. The actual title of the individual responsible for overall BSA

---

[111] 12 CFR 208.63(c)(3), (Federal Reserve); 12 CFR 326.8(c)(3) (FDIC); 12 CFR 748.2(c)(3) (NCUA); 12 CFR 21.21(d)(3) (OCC).

[112] FinCEN, "Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance" (August 2014).

compliance is not important; however, the individual's authority, independence, and access to resources within the DD is critical.

Indicators of appropriate authority of the BSA compliance officer may include senior management seeking the BSA compliance officer's input regarding: the ML/TF and other illicit financial activity risks related to expansion into new products, services, customer types, transactions, distribution channels, and geographic locations; or operational changes, such as the implementation of, or adjustments to, systems that impact the BSA compliance function. Refer to *3.5. New Products, Processes, and Technologies* for additional information. Indicators of appropriate independence of the BSA compliance officer may include, but are not limited to: clear lines of reporting and communication ultimately up to the board of directors or a designated board committee that do not compromise the BSA compliance officer's independence, the ability to undertake the BSA compliance officer's role without undue influence from the DD's business lines, identification and reporting of issues to senior management and the board of directors, and access as appropriate between the Department and the designated AML officer to address any identified issues with the AML/CFT Compliance Program, including status of any remediation.

The BSA compliance officer should have access to suitable resources. This may include, but is not limited to: adequate staffing with the skills and expertise necessary for the DD's overall risk level (based on products, services, customers, transactions, distribution channels, and geographic locations), size or complexity, and organizational structure; and systems to support the timely identification, measurement, monitoring, reporting, and management of the DD's ML/TF and other illicit financial activity risks. This could include adequate resources around regulatory change management for any updates within the United States or other jurisdictions that may impact the DD's risk profile or compensating controls (i.e., to keep up to date with the continuously evolving digital assets landscape), as well as trained investigators with experience in blockchain analytics.

Examiners should confirm that the DD's board of directors has designated an individual or individuals responsible for the overall AML/CFT compliance program who are appropriately qualified. Examiners should review reports to the board of directors and senior management regarding the status of ongoing compliance and pertinent BSA-related information, including the required notification of SAR filings and other key metrics around the DD's AML/CFT Compliance Program. Examiners should confirm that the BSA compliance officer has the appropriate authority, independence, and access to resources.

2.3.4.1. BSA Compliance Officer Examination Procedures

Objective: *Confirm that the DD's board of directors has designated a qualified individual or individuals (BSA compliance officer) responsible for coordinating and monitoring day-to-day compliance with BSA regulatory requirements. Determine whether the BSA compliance officer has the appropriate authority, independence, access to resources, and competence to effectively execute all duties.*

Procedure	Comments
1. Confirm that the DD's board of directors has designated an individual or individuals responsible for the overall AML/CFT compliance program.	
2. Confirm that the BSA compliance officer regularly updates the board of directors and senior management about the status of ongoing compliance with the BSA and pertinent BSA-related information, including the required notification of SAR filings.	
3. Determine whether the BSA compliance officer is competent, as demonstrated by knowledge of the BSA and related regulations, implementation of the DD's AML/CFT compliance program, and understanding of the DD's ML/TF and other illicit financial activity risk profile associated with its activities, including appropriate digital assets background and expertise. This may include evaluating which qualifications and/or certifications the BSA compliance officer holds.	
4. Determine whether the BSA compliance officer has the appropriate authority.	
5. Determine whether the BSA compliance officer has the appropriate independence. Indicators of appropriate independence may include, but are not limited to: • Clear lines of reporting and communication ultimately up to the board of directors, or a designated board	

Procedure	Comments
committee, which do not compromise the BSA compliance officer's independence. • The ability to undertake the BSA compliance officer's role without undue influence from the DD's business lines. • Identification and reporting of issues to senior management and the board of directors.	
6. Determine whether the BSA compliance officer has access to suitable resources. Indicators of suitable resources may include, but are not limited to: • Adequate staffing with the skills and expertise for the DD's overall risk level (based on products, services, customers, transactions, distribution channels, and geographic locations), size or complexity, and organizational structure. • Established processes/mechanisms to keep up to date with changes in regulation and industry practice (e.g., in the evolving digital assets environment). • Development of documented resourcing and succession plans (e.g., identification of key person risk and who would take over the role of the BSA compliance officer if the BSA compliance officer should leave the DD or take an extended leave of absence). • Systems to support the identification, measurement, monitoring, reporting, and management of the DD's ML/TF and other illicit financial activity risks, such as blockchain analytics and artificial intelligence/use of "big data."	

2.3.5. AML/CFT Training

Objective: *Confirm that the DD has developed a AML/CFT training program and delivered training to appropriate personnel.*

DDs must provide training for appropriate personnel.[113] Training should cover the aspects of the BSA that are relevant to the DD (including digital assets) and its risk profile, and appropriate personnel includes those whose duties require knowledge or involve some aspect of AML/CFT compliance. Training should cover BSA regulatory requirements, supervisory guidance, and the DD's internal AML/CFT policies, procedures, and processes. Training should be tailored to each individual's specific responsibilities, as appropriate. In addition, targeted training may be necessary for specific ML/TF and other illicit financial activity risks and requirements applicable to certain business lines or operational units, such as lending, trust services, foreign correspondent banking, and private banking. Given the unique nature of digital assets products and services, the DD should be aware of the prevailing techniques, methods, and trends in money laundering applicable the DD's risk profile (including its products, services, customers, distribution channels, business partners, and the level of complexity of its transactions). DDs should ensure that AML/CFT training is updated on an ongoing basis to account for the evolving digital assets environment, including new money laundering typologies and trends employed by illicit actors (e.g., the use of mixers & tumblers, anonymity enhanced cryptocurrencies ("AECs"), decentralized exchanges ("DEXs")/peer-to-peer ("P2P") exchanges with few BSA controls, chain-hopping[114], darknet marketplace, the deliberate misuse of legal entities and arrangements for facilitating money laundering and other illicit financial activity,[115] and high-risk geographies for ransomware[116] and other crimes) as well as associated blockchain analytics investigative techniques. For example, digital asset analytics providers often provide training relating to these topics and applications of their solutions to address digital asset-specific typologies and red flags, and may also offer certifications. A DD should consider whether its overall training is sufficient even if it relies on outside training. An overview of the purposes of the BSA and its regulatory requirements are typically provided to new staff during employee orientation or reasonably thereafter. The BSA compliance officer and BSA compliance staff should receive periodic

[113] 12 CFR 208.63(c)(4) (Federal Reserve); 12 CFR 326.8(c)(4) (FDIC); 12 CFR 748.2(c)(4) (NCUA); 12 CFR21.21(d)(4) (OCC).

[114] Chain-hopping is the practice of converting one form of cryptocurrency into another and moving one's funds from one blockchain to another; it is sometimes used by illicit actors as a layering technique in money laundering and other financial crimes.

[115] U.S. Department of the Treasury, "National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing" (March 2022).

[116] FinCEN, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" (November 2021).

training that is relevant and appropriate to remain informed of changes to regulatory requirements and changes to the DD's risk profile.

The board of directors and senior management should receive foundational training and be informed of changes and new developments in the BSA, including its implementing regulations, the federal banking agencies' regulations, the Department' rule-making, and supervisory guidance applicable to digital assets, as well as emergent industry guidance or regulations from other supervisory bodies that may be appropriate based on the DD's risk profile. While the board of directors may not require the same degree of training as banking operations personnel, the training should provide board members with sufficient understanding of the DD's risk profile and BSA regulatory requirements. Without a general understanding of the BSA, it is more difficult for the board of directors to provide adequate oversight of the AML/CFT compliance program, including approving the written AML/CFT compliance program, establishing appropriate independence for the AML/CFT compliance function, and providing sufficient AML/CFT resources.

Periodic training for appropriate personnel should incorporate current developments and changes to BSA regulatory requirements; supervisory guidance; internal policies, procedures, and processes; and the DD's products, services, customers, transactions, distribution channels, and geographic locations. Changes to information technology sources, systems, and processes used in BSA compliance may be covered during training for appropriate personnel. For example, the DD should assess the degree to which the DD has specialized training around use of any digital asset vendor tools as appropriate. The training program may be used to reinforce the importance that the board of directors and senior management place on the DD's compliance with the BSA and that all employees understand their role in maintaining an adequate AML/CFT compliance program.

Training programs should include examples of money laundering and suspicious activity monitoring and reporting that are tailored, as appropriate, to each operational area. Where the DD offers digital asset-specific activity that may pose a heightened risk, such as the on-ramp of different types of virtual currencies or activity that may involve anonymity-enhancing features, examiners should assess the business line documentation and training that is in place to address such risks, as well as compliance testing and audit reviews as appropriate based on the risks of the activity. In addition, given the recent increase in the use of digital assets to collect ransomware payments via unhosted wallets,[117] examiners should assess the documentation and training that is in place to address such new and emerging risks. According to the March 2022 *U.S. Treasury National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing*,[118] "the deliberate misuse of legal entities and arrangements, including limited liability

[117] FATF, "Second 12 Month Review of Revised FATF Standards - Virtual Assets and VASPs" (July 2021).

[118] U.S. Treasury, "National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing" (March 2022).

companies and other corporate vehicles, trusts, partnerships, and the use of nominees, continue to be significant tools for facilitating money laundering and other illicit financial activity in the U.S. financial system." Therefore, the DD should consider incorporating training on legal entities and other similar arrangements in AML/CFT training—particularly focusing on red flags associated with such deliberate misuse and the appropriate escalation/reporting process for front line/business staff. The DD should provide training for any agents who are responsible for conducting BSA-related functions on behalf of the DD. If the DD relies on another financial institution or other party to perform training, appropriate documentation should be maintained.[119]

DDs should document their training programs. Training and testing materials (if training- related testing is used by the DD), and the dates of training sessions should be maintained by the DD. Additionally, training materials and records should be available for auditor or examiner review. The DD should maintain documentation of attendance records and any failures of personnel to take the required training in a timely manner, as well as any corrective actions taken to address such failures, including escalations.

Examiners should determine whether all personnel whose duties require knowledge of the BSA are included in the training program and whether materials include training on BSA regulatory requirements, supervisory guidance, and the DD's internal AML/CFT policies, procedures, and processes. Moreover, examiners should determine whether the DD's training program appropriately captures the unique risks associated with digital assets, including common red flags, high risk customer types, and internal escalation pathways in the event that unusual activity is identified.

[119] For more information on collaborative arrangements, see "Interagency Statement on Sharing Bank Secrecy Act Resources," issued by Federal Reserve, FDIC, FinCEN, NCUA, and OCC (October 3, 2018).

2.3.5.1. AML/CFT Training Examination Procedures

Objective: *Determine whether the DD has developed a AML/CFT training program and delivered training to appropriate personnel.*

Procedure	Comments
1. Determine whether all personnel whose duties require knowledge of the BSA are included in the training program, that the BSA compliance officer and BSA compliance staff have received periodic training that is relevant and appropriate, and that the board of directors receives appropriate training that may include changes or new developments in the BSA.	
2. Determine whether the DD's training program materials address: • The importance that the board of directors and senior management place on ongoing education, training, employee accountability, and compliance. • Results of previous findings of noncompliance with internal policies and regulatory requirements, if applicable. • An overview of the purposes of the BSA and its regulatory requirements, supervisory guidance, and the DD's internal policies, procedures, and processes. • Different forms of ML/TF and other illicit financial activity risks as they relate to identification and examples of suspicious activity. This includes recent typologies or trends used by illicit actors and red flags for employees to identify and appropriately escalate such activity (e.g., for ransomware payments, deliberate misuse of legal entities and arrangements such as trusts for money laundering and other financial crimes). For example, the Department should assess where the DD offers digital asset-specific activity that may pose a	

Procedure	Comments
heightened risk to evaluate what specific training modules or certifications DD employees should have to demonstrate a nuanced understanding of risks specific to that higher risk product or service, including any specifics around the digital assets offered for that product or service. • Information tailored to specific risks of individual business lines or operational units. • Information on current developments and changes to the BSA regulatory requirements, as well as relevant recent regulatory and/or industry guidance and relevant industry developments. • Adequate training for any agents who are responsible for conducting BSA-related functions on behalf of the DD. This could include any digital asset-specific training (e.g., use of digital asset analytics tools) for specialized employees and training for third parties that perform discrete BSA-related functions (such as managed services and business process outsourcing firms).	
3. Determine whether the DD maintains documentation of the dates of training sessions and training and testing materials (if testing is used by the DD). Documentation should include attendance records and any failures of personnel to take the requisite training in a timely manner, as well as any corrective actions taken to address such failures.	
4. Determine whether the DD has developed governance documentation for BSA-related training (e.g., training policy, training needs assessment, annual training plan) and assess the quality of the DD's training records.	

Procedure	Comments
5. Determine whether any BSA-related training is outsourced to a third party (e.g., the use of a vendor for training material and/or delivery). To the extent third parties are used, evaluate whether the DD has a formalized governance process (e.g., including the review of such training content before it is delivered to DD employees).	

2.4. Assessing the OFAC Compliance Program

2.4.1. Office of Foreign Assets Control — Overview

Objective. *Assess the DD's risk-based OFAC compliance program to evaluate whether it is appropriate for the DD's OFAC risk, taking into consideration its products, services, customers, entities, transactions, and geographic locations.*

OFAC is an office of the U.S. Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted individuals and entities such as foreign countries, regimes, terrorists, international narcotics traffickers, and those engaged in certain activities such as the proliferation of weapons of mass destruction or transnational organized crime.

OFAC acts under Presidential wartime and national emergency powers, as well as various authorities granted by specific legislation, to impose controls on transactions and to freeze assets under U.S. jurisdiction. OFAC has been delegated responsibility by the Secretary of the Treasury for developing, promulgating, and administering U.S. sanctions programs.[120] Many of these sanctions are based on United Nations and other international mandates; therefore, they are multilateral in scope, and involve close cooperation with allied governments. Other sanctions are specific to the national security interests of the United States.

On November 9, 2009, OFAC issued a final rule entitled "Economic Sanctions Enforcement Guidelines" in order to provide guidance to persons subject to its regulations. The document explains the procedures that OFAC follows in determining the appropriate enforcement response to apparent violations of its regulations. Some enforcement responses may result in the issuance of a civil penalty that, depending on the sanctions program affected, may be as much as $250,000 per violation or twice the amount of a transaction, whichever is greater. The Guidelines outline the various factors that OFAC takes into account when making enforcement determinations, including the adequacy of a compliance program in place within an institution to ensure compliance with OFAC regulations.[121] In addition, OFAC has stated that it may impose civil penalties for sanctions violations under strict liability (a U.S. person may be held civilly liable for sanctions violations

---

[120] Trading With the Enemy Act (TWEA), 50 USC App 1-44; International Emergency Economic Powers Act (IEEPA), 50 USC 1701 *et seq.*; Antiterrorism and Effective Death Penalty Act (AEDPA), 8 USC 1189, 18 USC 2339B; United Nations Participation Act (UNPA), 22 USC 287c; Cuban Democracy Act (CDA), 22 USC 6001–10; The Cuban Liberty and Democratic Solidarity Act (Libertad Act), 22 USC 6021–91; The Clean Diamonds Trade Act, Pub. L. No. 108-19; Foreign Narcotics Kingpin Designation Act (Kingpin Act), 21 USC 1901–1908, 8 USC 1182; Burmese Freedom and Democracy Act of 2003, Pub. L. No. 108–61, 117 Stat. 864 (2003); The Foreign Operations, Export Financing and Related Programs Appropriations Act, Sec 570 of Pub. L. No. 104-208, 110 Stat. 3009-116 (1997); The Iraqi Sanctions Act, Pub. L. No. 101-513, 104 Stat. 2047-55 (1990); The International Security and Development Cooperation Act, 22 USC 2349 aa8–9; The Trade Sanctions Reform and Export Enhancement Act of 2000, Title IX, Pub. L. No. 106-387 (October 28, 2000).

[121] Refer to 73 *Fed. Reg.* 57593 (November 9, 2009) for additional information (also available on the OFAC Web site).

even without having knowledge or reason to know it was engaging in such a violation). As a general matter, however, OFAC takes into consideration the totality of facts and circumstances surrounding an apparent violation to determine the appropriate enforcement response. For example, OFAC may consider as mitigating factors a virtual currency company's implementation of a risk-based OFAC compliance program and remedial measures taken in response to an apparent violation."[122] For example, OFAC states that "while the resolution of each potential enforcement matter depends on the specific facts and circumstances, OFAC would be more likely to resolve apparent violations involving ransomware attacks with a non-public response (i.e., a No Action Letter or a Cautionary Letter) when the affected party took mitigating steps, particularly reporting a ransomware attack to law enforcement as soon as possible and providing ongoing cooperation."[123]

All U.S. persons,[124] including U.S. banks, bank holding companies, and nonbank subsidiaries, must comply with OFAC's regulations.[125] The federal banking agencies and the Department evaluate OFAC compliance programs to ensure that all banks subject to their supervision comply with the sanctions.[126] Unlike the BSA, the laws and OFAC-issued regulations apply not only to U.S. banks, their domestic branches, agencies, and international banking facilities, but also to their foreign branches, and often overseas offices and subsidiaries. OFAC encourages banks to take a risk-based approach to designing and implementing an OFAC compliance program.

On May 2, 2019, OFAC published *A Framework for OFAC Compliance Commitments* to provide organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States or U.S. persons, or that use U.S.-origin goods or services, with OFAC's perspective on the essential components of a sanctions compliance program.[127] The document also outlines how OFAC may incorporate these components into its evaluation of apparent violations and resolution of investigations resulting in settlements. Finally, the document includes an appendix that offers a brief analysis of some of the root causes of apparent violations of U.S. economic and trade sanctions programs OFAC has identified during its investigative process.

---

[122] OFAC, "Sanctions Compliance Guidance for Virtual Currency Industry" (October 2021).

[123] OFAC, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (September 2021).

[124] All U.S. persons must comply with OFAC regulations, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, all U.S. incorporated entities and their foreign branches. In the case of certain programs, such as those regarding Cuba and North Korea, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S. origin goods to comply.

[125] Additional information is provided in Foreign Assets Control Regulations for the Financial Community, which is available on the OFAC Web site.

[126] 31 CFR Chapter V.

[127] OFAC, "A Framework for OFAC Compliance Commitments" (May 2019).

In October 2021, OFAC issued the *Sanctions Compliance Guidance for Virtual Currency Industry* to emphasize that OFAC sanctions compliance obligations apply equally to transactions involving virtual currencies and those involving traditional fiat currencies. Similar to traditional financial institutions, digital asset firms are responsible for ensuring that they do not engage, directly or indirectly, in transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade- or investment-related transactions.[128]

The OFAC guidance outlined several elements to establish a strong sanctions compliance program, including implementing internal controls (e.g., geolocation and IP address blocking tools, VPN monitoring) and policies and procedures (e.g., for blocking and reporting requirements), and noted increased sanctions risk resulting from delayed compliance by some members of the digital assets industry that have not implemented an adequate sanctions compliance program before (or even years after) commencing operations.[129]

FinCEN reinforced OFAC's position as it relates to digital assets sanctions risk by noting that sanctioned persons and their counterparts may use digital assets and anonymizing tools to evade U.S. sanctions and protect their assets.[130]

In general, the regulations that OFAC administers require banks to do the following:

- Block accounts and other property of specified countries, entities, and individuals.
- Prohibit or reject unlicensed trade and financial transactions (including transactions involving digital assets) with specified countries, entities, and individuals.

Though not explicitly required by specific federal regulation, but as a matter of sound banking practice and in order to mitigate the risk of noncompliance with OFAC requirements, the Department requires DDs to establish and maintain an effective, written OFAC compliance program that is commensurate with their OFAC risk profile (based on products, services, customers, geographic locations, and other factors such as delivery channels as warranted based on the DD's risk profile). The program should identify higher-risk areas, provide for appropriate internal controls for screening and reporting, establish independent testing for compliance, designate a DD employee or employees as responsible for OFAC compliance, and create training programs for appropriate personnel in all relevant areas of the DD. Furthermore, a DD's OFAC compliance program should have controls that consider recent regulatory guidance, as well as relevant industry guidance. For example, in an advisory published in March 2022, FinCEN "[alerted] all financial institutions to be vigilant against efforts to evade the expansive sanctions and other U.S.-imposed restrictions [recently] implemented,"[131] DDs should,

---

[128] OFAC, "Sanctions Compliance Guidance for Virtual Currency Industry" (October 2021).

[129] OFAC, "Sanctions Compliance Guidance for Virtual Currency Industry" (October 2021).

[130] FinCEN, "FinCEN Advises Increased Vigilance for Potential Russia Sanctions Evasion Attempts" (March 2022).

[131] "E.O. 14024 specifically allows for the targeting of persons engaged in deceptive or structured transactions or dealings to circumvent any United States sanctions, including through the use of digital currencies or assets or the

therefore, be aware of timely OFAC/sanctions changes or advisories and any updates they need to make to their sanctions compliance program, as a result.

OFAC similarly encourages organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States, U.S. persons, or using U.S.-origin goods or services, "to employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating a sanctions compliance program (SCP)."

While each risk-based SCP will vary depending on a variety of factors—including the company's size and sophistication, products and services, customers and counterparties, and geographic locations—the Department considers OFAC guidance in its assessment of DDs, including addressing the five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.[132] The following sections provide overviews of how Department examiners evaluate DDs against these essential components.

Blocked Transactions

U.S. law requires that assets and accounts of an OFAC-specified country, entity, or individual be blocked when such property is located in the United States, is held by U.S. individuals or entities, or comes into the possession or control of U.S. individuals or entities. For example, if a funds transfer comes from offshore and is being routed through a U.S. bank to an offshore bank, and there is an OFAC-designated party to the transaction, it must be blocked. The definition of assets and property is broad and is specifically defined within each sanction program. As OFAC has clarified,[133] these obligations are the same, regardless of whether a transaction is conducted via digital assets or traditional fiat currency. Assets and property include anything of direct, indirect, present, future, or contingent value (including all types of bank transactions). Banks must block transactions that:

- Are by or on behalf of a blocked individual or entity;
- Are to or go through a blocked entity; or
- Are in connection with a transaction in which a blocked individual or entity has an interest.

For example, if a U.S. bank receives instructions to make a funds transfer payment that falls into one of these categories, it must execute the payment order and place the funds into a blocked

---

use of physical assets." FinCEN, "FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts" (March 2022).

[132] OFAC, "A Framework for OFAC Compliance Commitments" (May 2019).

[133] See OFAC's "Questions on Virtual Currency" section under OFAC FAQs: Sanctions Compliance.

account.[134] A payment order cannot be canceled or amended after it is received by a U.S. bank in the absence of an authorization from OFAC.

In the case of blocked transactions related to digital currency, OFAC has provided guidance on measures to follow:

> Once a U.S. person determines that they hold virtual currency that is required to be blocked pursuant to OFAC's regulations, the U.S. person must deny all parties access to that virtual currency, ensure that they comply with OFAC regulations related to the holding and reporting of blocked assets, and implement controls that align with a risk-based approach. U.S. persons are not obligated to convert the blocked virtual currency into traditional fiat currency (e.g., U.S. dollars) and are not required to hold such blocked property in an interest-bearing account. Blocked virtual currency must be reported to OFAC within 10 business days, and thereafter on an annual basis, so long as the virtual currency remains blocked.[135]

Prohibited Transactions

In some cases, an underlying transaction may be prohibited, but there is no blockable interest in the transaction (i.e., the transaction should not be accepted, but there is no OFAC requirement to block the assets). In these cases, the transaction is simply rejected, (i.e., not processed). For example, the Sudanese Sanctions Regulations prohibit transactions in support of commercial activities in Sudan. Therefore, a U.S. bank would have to reject a funds transfer between two companies, which are not Specially Designated Nationals or Blocked Persons (SDN), involving an export to a company in Sudan that also is not an SDN. Because the Sudanese Sanctions Regulations would only require blocking transactions with the Government of Sudan or an SDN, there would be no blockable interest in the funds between the two companies. However, because the transactions would constitute the exportation of services to Sudan, which is prohibited, the U.S. bank cannot process the transaction and would simply reject the transaction.

Similarly, if the DD received a virtual currency funds transfer request from an IP address within a country subject to comprehensive sanctions, even which does not involve an SDN, that transaction should be rejected. Accordingly, examiners should assess the degree to which the DD's processes in place are able to validate the legitimacy of the user as well as the user's access credentials, geolocation, IP address, use of VPN, device, and generally, their identity. Where the DD leverages vendor solutions (e.g., through a digital asset analytics provider or OFAC compliance vendor), the DD should demonstrate how the solution integrates into the DD's overall control framework, with clearly delineated accountability for IP address verification. IP address verification should also include periodic data updates, as appropriate, and processes to account for DD software updates and architecture changes. For example, this could include IP address blocking reports, and systems configurations testing to verify that the IP verification

---

[134] A blocked account is a segregated interest-bearing account (at a commercially reasonable rate), which holds the customer's property until the target is delisted, the sanctions program is rescinded, or the customer obtains an OFAC license authorizing the release of the property.

[135] OFAC, "Sanctions Compliance Guidance for Virtual Currency Industry" (October 2021).

reviews and other control measures are functioning as intended. As part of this review, examiners may assess the DD's processes in place to reject or hold transactions, confer with OFAC and the Department for guidance as appropriate, and any other appropriate escalation measures.

It is important to note that the OFAC regime specifying prohibitions against certain countries, entities, and individuals is separate and distinct from the provision within the BSA's CIP regulation (31 CFR 1020.220(a)(4)) that requires banks to compare new accounts against government lists of known or suspected terrorists or terrorist organizations within a reasonable period of time after the account is opened. OFAC lists have not been designated government lists for purposes of the CIP rule. Refer to the core overview section, "Customer Identification Program," page 47 of the FFIEC AML Manual, for further guidance.

OFAC explains that "as a general matter, U.S. persons and persons otherwise subject to OFAC jurisdiction, including firms that facilitate or engage in online commerce or process transactions using digital currency [or digital assets], are responsible for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade or investment-related transactions. Prohibited transactions include transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC under various sanctions authorities. Additionally, persons that provide financial, material, or technological support for or to a designated person may be designated by OFAC under the relevant sanctions authority."[136]

OFAC Licenses

OFAC has the authority, through a licensing process, to permit certain transactions that would otherwise be prohibited under its regulations. OFAC can issue a license to engage in an otherwise prohibited transaction when it determines that the transaction does not undermine the U.S. policy objectives of the particular sanctions program, or is otherwise justified by U.S. national security or foreign policy objectives. OFAC can also promulgate general licenses, which authorize categories of transactions, such as allowing reasonable service charges on blocked accounts, without the need for case-by-case authorization from OFAC. These licenses can be found in the regulations for each sanctions program (31 CFR, Chapter V (Regulations)) and may be accessed from the OFAC Web site. Before processing transactions that may be covered under a general

[136] See OFAC's "Questions on Virtual Currency" section under OFAC FAQs: Sanctions Compliance as well as FinCEN's "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 9, 2019) for more information.

license, DDs should verify that such transactions meet the relevant criteria of the general license.[137]

Specific licenses are issued on a case-by-case basis.[138] A specific license is a written document issued by OFAC authorizing a particular transaction or set of transactions generally limited to a specified time period. To receive a specific license, the person or entity who would like to undertake the transaction must submit an application to OFAC. If the transaction conforms to OFAC's internal licensing policies and U.S. foreign policy objectives, the license generally is issued. If a DD's customer claims to have a specific license, the DD should verify that the transaction conforms to the terms and conditions of the license (including the effective dates of the license), and it may wish to obtain and retain a copy of the authorizing license for recordkeeping purposes.

OFAC Reporting

Banks must report all blocking activity to OFAC within 10 business days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30).[139] Once assets or funds are blocked, they should be placed in a separate blocked account. DDs should have clearly documented processes, policies, and procedures for how they will maintain blocked activities including each type of digital asset offering. DDs should also have procedures and processes clarifying when it is appropriate to submit blocking reports to OFAC in addition to filing SARs with FinCEN (e.g., for the same activity or customer) so as to ensure compliance with OFAC reporting requirements.[140] Prohibited transactions that are rejected must also be reported to OFAC within 10 business days of the occurrence.[141]

Banks must keep a full and accurate record of each rejected transaction for at least five years after the date of the transaction. For blocked property (including blocked transactions), records must be maintained for the period the property is blocked and for five years after the date the property is unblocked.

---

[137] License information for a particular sanction program is available on the OFAC Web site or by contacting OFAC's Licensing area at (202) 622-2480.

[138] Applications for a specific license may be submitted either online from the OFAC Web site, or in writing to: Licensing Department, Office of Foreign Assets Control, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

[139] The annual report is to be filed on form TD F 90-22.50.

[140] FinCEN, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" (November 2021).

[141] Reporting, procedures, and penalties regulations, 31 CFR Part 501.

Additional information concerning OFAC regulations, such as Sanctions Program and Country Summaries brochures; the SDN and other lists, including both entities and individuals; recent OFAC actions; and "Frequently Asked Questions," can be found on the OFAC Web site.[142]

Voluntary Self Disclosures

Per OFAC:

> [A] company can and is encouraged to voluntarily disclose a past violation. Self-disclosure is considered a mitigating factor by OFAC in Civil Penalty proceedings. A self-disclosure should be in the form of a detailed letter, with any supporting documentation, to Compliance and Enforcement Department, Director, Office of Foreign Assets Control, U.S. Department of the Treasury, 1500 Pennsylvania Ave., N.W., Washington, DC 20220. OFAC does not have an "amnesty" program. The ramifications of non-compliance, inadvertent or otherwise, can jeopardize critical foreign policy and national security goals. OFAC does, however, review the totality of the circumstances surrounding any violation, including the quality of a company's OFAC compliance program. [11-16-07]

In the event that a company identifies previously undetected violations of OFAC regulations for completed transactions, the Department generally requires disclosure of all material information relating to violations to both the Department and OFAC in a timely manner. Questions surrounding disclosure should be addressed to the Department and OFAC on a confidential basis.

[142] This information is available on the OFAC Web site, or by contacting OFAC's hot line at (202) 622-2490 or toll-free at (800) 540-6322.

2.4.1.1. Office of Foreign Assets Control – Examination Procedures

Objective. *Assess the DD's risk-based Office of Foreign Assets Control (OFAC) compliance program to evaluate whether it is appropriate for the DD's OFAC risk, taking into consideration its products, services, customers, entities, transactions, and geographic locations*.

Procedure	Comments
1. Review the DD's written OFAC compliance program in the context of the DD's OFAC risk assessment. Consider the following: • When the written OFAC compliance program was developed and implemented (i.e., ensure OFAC compliance program is in place prior to approving charter application and before DD's operational date). • The process used to block and reject transactions for each type of digital asset that the DD offers. • The process used to inform management of blocked or rejected transactions as well as any other OFAC-related key performance indicators ("KPIs") or key risk indicators ("KRIs"). • The adequacy and timeliness of filings to both the Department and OFAC, including self-disclosures, responsible parties for filings, and escalation processes in place. • The process to manage blocked accounts (such accounts must be reported to OFAC). • The processes and procedures in place to ensure compliance with all OFAC reporting requirements, including the need to submit blocking reports to OFAC in addition to filing SARs with FinCEN in certain cases. • The processes in place to validate that the user is not subject to sanctions, as well as the user's access credentials, geolocation, IP address, email address, use of VPN, device, and generally, their identity, including measures taken to ensure data accuracy. • The record retention requirements (e.g., five-year requirement to retain relevant OFAC records; for blocked property, record retention	

Procedure	Comments
for as long as blocked; once unblocked, records must be maintained for five years). • Documented process for voluntary self-disclosure filings with the Department and OFAC.	
Transaction Testing	
2. On the basis of a DD's risk assessment, prior examination reports, and a review of the DD's audit findings, select the following samples to test the DD's OFAC compliance program for adequacy, as follows: • Review a sample of potential OFAC matches and evaluate the DD's resolution for blocking and rejecting processes for each type of interdiction software the DD uses. • Review a sample of blocked and rejected reports filed with OFAC and evaluate their completeness and timeliness. • If the DD is required to maintain blocked accounts, select a sample and ensure that the DD maintains adequate records of amounts blocked and the ownership of blocked funds, and accurately reports required information on blocked property annually (by September 30) to OFAC. Test the controls in place to verify that the account is blocked. As warranted, review for blocked accounts of digital assets.	

2.4.2. OFAC Management Commitment

Objective. *Assess the DD's management commitment to the DD's OFAC compliance program to evaluate whether it is appropriate for the DD's OFAC risk, taking into consideration its products, services, customers, entities, transactions, distribution channels and geographic locations*.

Senior Management's commitment to, and support of, an organization's risk-based SCP is one of the most important factors in determining its success. This support is essential in ensuring the SCP receives adequate resources and is fully integrated into the organization's daily operations, and also helps legitimize the program, empower its personnel, and foster a culture of compliance throughout the organization.

General Aspects of an SCP: Senior Management Commitment

Senior management commitment to supporting an organization's SCP is a critical factor in determining the success of the SCP. Effective management support includes the provision of adequate resources to the compliance unit(s) and support for compliance personnel's authority within an organization. The term "senior management" may differ among various organizations, but typically the term should include senior leadership and executives. Elements of an appropriate SCP include the following:

I. Senior management has reviewed and approved the organization's SCP.

II. Senior management ensures that its compliance unit(s) is/are delegated sufficient authority and autonomy to deploy its policies and procedures in a manner that effectively controls the organization's OFAC risk. As part of this effort, senior management ensures the existence of direct reporting lines between the SCP function and senior management, including routine and periodic meetings between these two elements of the organization.

III. Senior management has taken, and will continue to take, steps to ensure that the organization's compliance unit(s) receive adequate resources—including in the form of human capital, expertise, information technology, and other resources, as appropriate—that are relative to the organization's breadth of operations, target and secondary markets, and other factors affecting its overall risk profile.

These efforts could generally be measured by the following criteria:

A. The organization has appointed a dedicated OFAC sanctions compliance officer[143];

B. The quality and experience of the personnel dedicated to the SCP, including: (i) the technical knowledge and expertise of these personnel with respect to OFAC's regulations, processes, and actions; (ii) the ability of these personnel to understand complex financial and commercial activities, apply their knowledge of OFAC to these items, and identify OFAC-related issues, risks, and prohibited activities; and (iii) the efforts to ensure that personnel dedicated to the SCP have sufficient experience and an appropriate position within the organization, and are an integral component to the organization's success.

C. Sufficient control functions exist that support the organization's SCP—including but not limited to information technology software and systems—that adequately address the organization's OFAC-risk assessment and levels.

IV. Senior management promotes a "culture of compliance" throughout the organization.

These efforts could generally be measured by the following criteria:

A. The ability of personnel to report sanctions related misconduct by the organization or its personnel to senior management without fear of reprisal.

B. Senior management messages and takes actions that discourage misconduct and prohibited activities, and highlight the potential repercussions of non-compliance with OFAC sanctions; and

C. The ability of the SCP to have oversight over the actions of the entire organization, including but not limited to senior management, for the purposes of compliance with OFAC sanctions.

D. Training.

V. Senior management demonstrates recognition of the seriousness of apparent violations of the laws and regulations administered by OFAC, or malfunctions, deficiencies, or failures by the organization and its personnel to comply with the SCP's policies and procedures, and implements necessary measures to reduce the occurrence of apparent violations in the future. Such measures should address the root causes of past apparent violations and represent systemic solutions whenever possible.

[143] This may be the same person serving in other senior compliance positions, e.g., the Bank Secrecy Act Officer or an Export Control Officer, as many institutions, depending on size and complexity, designate a single person to oversee all areas of financial crimes or export control compliance.

2.4.2.1. OFAC Management Commitment – Examination Procedures

Objective. *Assess the DD's management commitment to the DD's OFAC compliance program to evaluate whether it is appropriate for the DD's OFAC risk, taking into consideration its products, services, customers, entities, transactions, distribution channels and geographic locations*.

Procedure	Comments
1. Determine whether senior management of the DD has developed policies, procedures, and processes based on their risk assessment to ensure compliance with OFAC laws and regulations and the board of directors has approved such policies, procedures, and processes, as well as to consider applicable recent regulatory guidance and industry guidance.	
2. Determine whether the DD has dedicated adequate resources to its OFAC compliance program (e.g., an OFAC compliance officer). Both the number and qualifications (including both sanctions compliance and digital assets-related knowledge and experience) of resources should be considered.	
3. Determine whether roles and responsibilities of OFAC compliance resources are clearly delineated and, for one, clarify which member(s) of the OFAC compliance team are responsible for contacting OFAC and when it is appropriate to do so.	
4. Determine whether the DD has documented resourcing and succession plans (e.g., identification of key person risk and who would take over the role of the OFAC compliance officer if the OFAC compliance officer should leave the DD).	
5. Evaluate the processes/mechanisms used by the DD to keep up to date with changes in regulation and industry practice (e.g., in the evolving digital assets environment).	
6. Assess what steps the DD's management has taken to assess its commitment to OFAC compliance (e.g., through appropriate approvals, reporting lines, resourcing, communications, or trainings).	

2.4.3. OFAC Internal Controls

Objective. *Assess the DD's OFAC internal controls to evaluate whether it is appropriate for the DD's OFAC risk, taking into consideration its products, services, customers, entities, transactions, and geographic locations*.

An effective OFAC compliance program should include internal controls, including policies and procedures, to identify, interdict, escalate, report (as appropriate), and keep records pertaining to activity that may be prohibited by the regulations and laws administered by OFAC. The purpose of internal controls is to outline clear expectations, define procedures and processes pertaining to OFAC compliance (including reporting and escalation chains), and minimize the risks identified by the organization's risk assessments. Policies and procedures should be enforced, weaknesses should be identified (including through root cause analysis of any compliance breaches) and remediated, and internal and/or external audits and assessments of the program should be conducted on a periodic basis. Given the dynamic nature of U.S. economic and trade sanctions, a successful and effective SCP should be capable of adjusting rapidly to changes published by OFAC.[144] These include the following: (i) updates to OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List"[145]), the Sectoral Sanctions Identification List ("SSI List"), and other sanctions related lists; (ii) new, amended, or updated sanctions programs or prohibitions imposed on targeted foreign countries, governments, regions, or persons, through the enactment of new legislation, the issuance of new Executive orders, regulations, or published OFAC guidance or other OFAC actions; and (iii) the issuance of general licenses. Such a program should also have controls in place that consider applicable recent regulatory guidance, as well as industry guidance.

General Aspects of an SCP: Internal Controls

I. The organization has designed and implemented written policies and procedures outlining the SCP. These policies and procedures are relevant to the organization, capture the organization's day-to-day operations and procedures, are easy to follow, and designed to prevent employees from engaging in misconduct.

II. The organization has implemented internal controls that adequately address the results of its OFAC risk assessment and profile. These internal controls should enable the organization to clearly and effectively identify, interdict, escalate, and report to appropriate personnel within the organization transactions and activity that may be prohibited by OFAC. To the extent information technology solutions factor into the organization's internal controls, the organization has selected and calibrated the solutions in a manner that is appropriate to address the organization's risk profile and

[144] Accordingly, examiners may evaluate controls the bank has in place to conduct sanctions screening of changes and updates to customer names and associated parties for each product and service that the bank offers.

[145] Please see Treasury's site for a comprehensive OFAC SDN list.

compliance needs, and the organization routinely tests the solutions to ensure effectiveness.

III. The organization enforces the policies and procedures it implements as part of its OFAC compliance internal controls through internal and/or external audits.

IV. The organization ensures that its OFAC-related recordkeeping policies and procedures adequately account for its requirements pursuant to the sanctions programs administered by OFAC.

V. The organization ensures that, upon learning of a weakness in its internal controls pertaining to OFAC compliance, it will take immediate and effective action, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.

VI. The organization has clearly communicated the SCP's policies and procedures to all relevant staff, including personnel within the SCP program, as well as relevant gatekeepers and business units operating in high-risk areas (e.g., customer acquisition, payments, sales, etc.) and to external parties performing SCP responsibilities on behalf of the organization.

VII. The organization has appointed personnel for integrating the SCP's policies and procedures into the daily operations of the company or corporation. This process includes consultations with relevant business units and confirms that employees understand the policies and procedures.

Internal controls should include the following elements:

Identifying and reviewing suspect transactions. The DD's policies, procedures, and processes should address how the DD identifies and reviews transactions and accounts for possible OFAC violations, whether conducted manually, through interdiction software, or a combination of both. For screening purposes, the DD should clearly define its criteria for comparing names provided on the OFAC list with the names in the DD's files or on transactions and for identifying transactions or accounts involving sanctioned countries. The DD's policies, procedures, and processes should also address how the DD determines whether an initial OFAC hit is a valid match or a false hit.[146] A high volume of false hits may indicate a need to review the DD's interdiction program. Particularly where DDs leverage third party-vendors (e.g., digital asset analytics, artificial intelligence ("AI") or "big data" providers), the DD should have clearly auditable processes and metrics around alert dispositions, escalation processes, and data quality/updates.

[146] Due diligence steps for determining a valid match are provided in *Using OFAC's Hotline* on the OFAC Web site.

The screening criteria used by DDs to identify name variations and misspellings should be based on the level of OFAC risk associated with the particular product or type of transaction. For example, in a higher-risk area with a high-volume of transactions, the DD's interdiction software should be able to identify close name derivations for review. The SDN list attempts to provide name derivations; however, the list may not include all derivations. More sophisticated interdiction software may be able to catch variations of an SDN's name not included on the SDN list. Banks with lower OFAC risk and those with low volumes of transactions may decide to manually filter for OFAC compliance. Decisions to use interdiction software and the degree of sensitivity of that software should be based on a DD's assessment of its risk and the volume of its transactions. In determining the frequency of OFAC checks and the filtering criteria used (e.g., name derivations), DDs should consider the likelihood of incurring a violation and available technology. In addition, DDs should periodically reassess their OFAC filtering system. For example, if a DD identifies a name derivation of an OFAC target, then OFAC suggests that the DD add the name to its filtering process.

New accounts should be compared with the OFAC lists prior to being opened or shortly thereafter (e.g., during nightly processing). DDs that perform OFAC checks after account opening should have procedures in place to prevent transactions, other than initial deposits, from occurring until the OFAC check is completed. Prohibited transactions conducted prior to completing an OFAC check may be subject to possible enforcement action. In addition, DDs should have policies, procedures, and processes in place to check existing customers when there are additions or changes to the OFAC list. The frequency of the review should be based on the DD's OFAC risk. For example, DDs with a lower OFAC risk level may periodically (e.g., weekly, monthly, or quarterly) compare the customer base against the OFAC list. Transactions such as funds transfers, on-ramps, virtual currency exchange, off-ramps, digital assets escrow activity, stablecoin activity, and noncustomer transactions should be checked against OFAC lists. When developing OFAC policies, procedures, and processes, the DD should keep in mind that OFAC considers the continued operation of an account or the processing of transactions post-designation, along with the adequacy of the DD's OFAC compliance program, to be a factor in determining the appropriate enforcement response to an apparent violation of OFAC regulations.[147] The DD should maintain documentation of its OFAC checks on new accounts, the existing customer base, and specific transactions. In addition to the above, the Department should assess the degree to which DDs maintain independent, in-house (internal) lists of digital asset addresses the DD has decided not to establish or continue business relationships with due to suspicions of ML/TF or sanctions evasion. DDs should screen their customers and counterparties (i.e., other parties involved in a transaction) against such internally flagged addresses.[148]

---

[147] Refer to 74 *Fed. Reg.* 57593 (November 9, 2009), "Economic Sanctions Enforcement Guidelines." Further information is available on the OFAC Web site.

[148] See Recommendation 10 guidance on page 41 of "Guidance For a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (June 2019). "Independent, in-house lists" may include data obtained from vendors which is periodically updated by the bank to account for intelligence gained from customer relationships.

Per OFAC guidance, DDs should incorporate geolocation tools and IP address blocking controls to identify and prevent IP addresses that originate in sanctioned jurisdictions from accessing a company's website and services for activity that is prohibited by OFAC's regulations, and not authorized or exempt.[149]

DDs should leverage analytics tools to identify IP misattribution, for example, by screening IP addresses against known virtual private network (VPN) IP addresses and identifying improbable logins.[150] In addition, DDs would benefit from employing "transaction monitoring and investigation tools to continually review historical information for such addresses or other identifying information to better understand their exposure to sanctions risks and identify sanctions compliance program deficiencies."[151] Similarly, FinCEN provided guidance that emphasized the importance for digital assets firms to identify and timely report sanctions evasion suspicious activity and conduct necessary CDD/EDD[152] as well as to use information sharing (e.g., 314(b)) and automated tools/analytics for sanctions screening.

As an additional control, given that industry solutions have limited coverage of email address screening, several firms in the digital assets space have decided to develop and implement internal processes for email address monitoring (i.e., collecting, analyzing, and escalating email addresses that indicate a potential connection to a sanctioned individual, entity or jurisdiction, while noting that email addresses alone are not an adequate indicator of a sanction's nexus).

Furthermore, data from blockchain analytics providers points to outsized sanctions risks associated with stablecoins (e.g., given the appeal to illicit actors to use a less volatile form of cryptocurrency), emphasizing the need for blockchain analytics solutions—such as crypto wallet screening and crypto transaction monitoring—to assist DDs in complying with relevant U.S. and international sanctions.[153] Additionally, more digital assets firms are integrating real-time screening by establishing a direct connection between their blockchain analytics tools and their custody solutions/settlement systems to further bolster their OFAC screening capabilities and mitigate against the risk of deposits from and withdrawals to sanctioned entities.

If a DD uses a third party, such as an agent or service provider, to perform OFAC checks on its behalf, as with any other responsibility performed by a third party, the DD is ultimately responsible for that third party's compliance with the OFAC requirements. As a result, DDs should have a written agreement in place and establish adequate controls and review procedures

---

[149] OFAC, "Sanctions Compliance Guidance for Virtual Currency Industry" (October 2021).

[150] Ibid

[151] Ibid

[152] FinCEN, "FinCEN Advises Increased Vigilance for Potential Russia Sanctions Evasion Attempts" (March 2022).

[153] Elliptic, "Crypto Addresses Holding NFTs Worth $532k are Among the Latest Sanctioned by OFAC" (November 2021).

for such relationships. Refer to *3.8. Model Risk Management* for more information around control measure for models and vendor relationships.

Updating OFAC lists. A DD's OFAC compliance program should include policies, procedures, and processes for timely updating of the lists of sanctioned countries and blocked entities, and individuals, and disseminating such information throughout the DD's domestic operations and its offshore offices, branches and, in the case of Iran and Cuba, foreign subsidiaries. This would include ensuring that any manual updates of interdiction software are completed in a timely manner. For example, OFAC has designated several malicious cyber actors, including perpetrators and facilitators of ransomware.[154] Examiners should, therefore, assess how the DD ensures its OFAC/sanctions lists are kept up-to-date, especially with any recent trends and/or typologies in illicit activity, such as ransomware. Accordingly, examiners should evaluate the DD's sanctions list governance and sanctions list management process to determine the rationale behind lists used (including government-issued lists, subscription lists, and any internal lists—such as an internal keywords list of a sanctioned jurisdiction's cities and regions for screening KYC information) and update/maintenance procedures to form an overall view that it is consistent with the DD's risk profile.

Screening Automated Clearing House (ACH) transactions. ACH transactions may involve persons or parties subject to the sanctions programs administered by OFAC. Refer to the expanded overview section, "Automated Clearing House Transactions," page 216 of the FFIEC AML Manual, for additional guidance. OFAC has clarified its interpretation of the application of OFAC's rules for domestic and cross-border ACH transactions and provided more detailed guidance on international ACH transactions.[155]

With respect to domestic ACH transactions, the Originating Depository Financial Institution (ODFI) is responsible for verifying that the Originator is not a blocked party and making a good faith effort to ascertain that the Originator is not transmitting blocked funds. The Receiving Depository Financial Institution (RDFI) similarly is responsible for verifying that the Receiver is not a blocked party. In this way, the ODFI and the RDFI are relying on each other for compliance with OFAC regulations.

If an ODFI receives domestic ACH transactions that its customer has already batched, the ODFI is not responsible for unbatching those transactions to ensure that no transactions violate OFAC's regulations. If an ODFI unbatches a file originally received from the Originator in order to process "on-us" transactions, that ODFI is responsible for the OFAC compliance for the on-us transactions because it is acting as both the ODFI and the RDFI for those transactions. ODFIs acting in this capacity should already know their customers for the purposes of OFAC and other regulatory requirements. For the residual unbatched transactions in the file that are not "on-us," as well as

---

[154] OFAC, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (September 2021).

[155] U.S. Treasury Department, "Guidance to National Automated Clearing House Association (NACHA) on cross-border ACH" http://www.treasury.gov/resource-center/sanctions/Documents/gn121404.pdf (November 2004).

those situations where DDs deal with unbatched ACH records for reasons other than to strip out the on-us transactions, DDs should determine the level of their OFAC risk and develop appropriate policies, procedures, and processes to address the associated risks. Such policies might involve screening each unbatched ACH record. Similarly, DDs that have relationships with third- party service providers should assess those relationships and their related ACH transactions to ascertain the DD's level of OFAC risk and to develop appropriate policies, procedures, and processes to mitigate that risk.

With respect to cross-border screening, similar but somewhat more stringent OFAC obligations hold for International ACH transactions (IAT). In the case of inbound IATs, and regardless of whether the OFAC flag in the IAT is set, an RDFI is responsible for compliance with OFAC sanctions programs. For outbound IATs, however, the ODFI cannot rely on OFAC screening by an RDFI outside of the United States. In these situations, the ODFI must exercise increased diligence to ensure that illegal transactions are not processed.

Due diligence for an inbound or outbound IAT may include screening the parties to a transaction, as well as reviewing the details of the payment field information for an indication of a sanctions violation, investigating the resulting hits, if any, and ultimately blocking or rejecting the transaction, as appropriate. Refer to the expanded overview section, "Automated Clearing House Transactions," page 216 of the FFIEC AML Manual, for additional guidance.

Additional information on the types of retail payment systems (ACH payment systems) is available in the FFIEC *Information Technology Examination Handbook*.[156][163]

In guidance issued on March 10, 2009, OFAC authorized institutions in the United States when they are acting as an ODFI/Gateway Operator (GO) for inbound IAT debits to reject transactions that appear to involve blockable property or property interests.[157] The guidance further states that to the extent that an ODFI/GO screens inbound IAT debits for possible OFAC violations prior to execution and in the course of such screening discovers a potential OFAC violation, the suspect transaction is to be removed from the batch for further investigation. If the ODFI/GO determines that the transaction does appear to violate OFAC regulations, the ODFI/GO should refuse to process the transfer. The procedure applies to transactions that would normally be blocked as well as to transactions that would normally be rejected for OFAC purposes based on the information in the payment.

Reporting. An OFAC compliance program should also include policies, procedures, and processes for handling validly blocked or rejected items under the various sanctions programs. When there is a question about the validity of an interdiction, DDs can contact OFAC by phone or e-hot line for guidance. Most other items should be reported through usual channels within ten days of the occurrence. The policies, procedures, and processes should also address the

[156] Refer to the FFIEC *Information Technology Examination Handbook's Retail Payment Systems* booklet.

[157] Refer to the NACHA Web site.

management of blocked accounts. DDs are responsible for tracking the amount of blocked funds, the ownership of those funds, and interest paid on those funds. Total amounts blocked, including interest, must be reported to OFAC by September 30 of each year (information as of June 30). When a DD acquires or merges with another DD, both DDs should take into consideration the need to review and maintain such records and information. For both manual and automated reporting (i.e., using an MIS), DDs should develop and implement a written data governance program to ensure that the data feeding into various OFAC reports is accurate and consistent.

DDs no longer need to file SARs based solely on blocked narcotics- or terrorism-related transactions, as long as the DD files the required blocking report with OFAC. However, because blocking reports require only limited information, if the DD is in possession of additional information not included on the OFAC blocking report, a separate SAR should be filed with FinCEN that would include such information. In addition, the DD should file a SAR if the transaction itself would be considered suspicious in the absence of a valid OFAC match.[158] When filing OFAC/sanctions-related SARs, DDs should refer to FinCEN's specific advisories and key terms depending on the nature of the suspicious activity.[159]

Maintaining license information. OFAC recommends that DDs consider maintaining copies of customers' OFAC licenses on file. This allows the DD to verify whether a customer is initiating a legal transaction. DDS should also be aware of the expiration date on the OFAC license. If it is unclear whether a particular transaction would be authorized under the terms of the license, the DD should contact OFAC. Maintaining copies of OFAC licenses also is useful when another DD in the payment chain requests verification of a license's validity. Copies of OFAC licenses should be maintained for five years, following the most recent transaction conducted in accordance with the license.

Management Information ("MI") Reporting & Issues Management. An effective OFAC/sanctions compliance program should also include the derivation of key sanctions compliance risk metrics (e.g., KRIs and KPIs) and the production of regular reporting on such metrics, as well as transaction and trend analyses as they pertain to sanctions compliance. The scope of such sanctions compliance MI should also include the count of voluntary self-disclosures and sanctions alerts and positive hits, as well as a historical analysis/lookback of transaction activity after OFAC lists a virtual currency address on the SDN list to identify potential connections.[160] When using MIS, DDs should ensure they have developed and implemented a written data governance program for AML/CFT and OFAC/sanctions-related MI that feeds into various reporting. Additionally, an effective OFAC/sanctions program should include a formalized

---

[158] Refer to FinCEN Release Number 2004-02, *Unitary Filing of Suspicious Activity and Blocking Reports*, 69 *Fed. Reg.* 76847 (December 2004).

[159] FinCEN, "FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts" (March 2022).

[160] OFAC, "Sanctions Compliance Guidance for Virtual Currency Industry" (October 2021).

issues management process with written policies and procedures defining how to identify, escalate (or report), and remediate sanctions compliance-related issues.

2.4.3.1. OFAC Internal Controls – Examination Procedures

Objective. *Assess the DD's OFAC internal controls to evaluate whether it is appropriate for the DD's OFAC risk, taking into consideration its products, services, customers, entities, transactions, and geographic locations*.

Procedure	Comments
1. Review the DD's OFAC compliance program in the context of the DD's OFAC risk assessment. Consider the following: • When the DD's OFAC internal controls were developed and implemented (i.e., whether before the DD was operational). • The extent of, and method for, conducting OFAC searches of each relevant department or business line (e.g., on/off ramp of virtual currencies, escrow services, automated clearing house (ACH) transactions, cross-border funds transfers, trade finance products, monetary instrument sales, trusts, loans, deposits, and investments) as the process may vary from one department or business line to another. • The extent of, and method for, conducting OFAC searches of account parties other than accountholders, which may include beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories, and powers of attorney, including the frequency of review of such names against updates to sanctions lists. • The assignment of responsibilities within the institution for ensuring compliance with OFAC. • Timeliness of obtaining and updating OFAC lists and filtering criteria. • The appropriateness of the filtering criteria used by the DD to reasonably identify OFAC matches (e.g., the extent to which the filtering or search criteria includes misspellings and name derivations). • The processes and tools (e.g., blockchain analytics, artificial intelligence or "big data" providers) for identifying and preventing individuals/entities from sanctioned	

Procedure	Comments
jurisdictions or associated with sanctioned persons, entities, etc., from accessing the DD's products and services (e.g., sanctions screening, PEP screening, adverse media screening, IP address and geo-location blocking, VPN monitoring, email address monitoring, etc.). • Whether the DD has formal processes and procedures outlining OFAC requirements related to recordkeeping and reporting (e.g., with respect to blocking and rejecting, voluntary self-disclosures, annual blocked property reports, etc.). • Whether the DD has formal processes and procedures related to management information reporting and issues management, specifically for OFAC/sanctions compliance. This includes evaluating whether the DD has a written data governance program for AML/CFT and OFAC/sanctions-related MIS that feeds into various reporting. • Whether the DD has a process in place for reviewing and updating end-user agreements to include information about U.S. sanctions requirements. • The process used to investigate potential matches, including escalation procedures for potential matches.	
2. Assess the DD's sanctions list governance and sanctions list management process, including the rationale behind the scope of lists used (including government-issued lists, subscription lists, and any internal lists—such as a keywords list of a sanctioned jurisdiction's cities and regions for screening Know-Your-Customer information), updates/maintenance, frequency of reviews, including appropriate management sign-offs, and form an overall view of whether it is consistent with the DD's risk profile.	
3. Determine whether the DD has adequately addressed weaknesses or deficiencies identified by OFAC, auditors, or regulators.	

Procedure	Comments
Transaction Testing	
4. On the basis of a DD's risk assessment, prior examination reports, and a review of the DD's audit findings, select the following samples to test the DD's OFAC compliance program for adequacy, as follows: • Sample new accounts (e.g., on-ramps, virtual currency exchange, off-ramps, digital assets escrow activity, stablecoin network participants, deposit, loan, trust, safe deposit, investments) and evaluate the filtering process used to search the OFAC database (e.g., the timing of the search), and documentation maintained evidencing the searches for each type of product. • Sample appropriate transactions that may not be related to an account (e.g., funds transfers, digital asset escrow activity, monetary instrument sales, and check-cashing transactions), and evaluate the filtering criteria used to search the OFAC database, the timing of the search, and documentation maintained evidencing the searches. • If the DD uses an automated system to conduct searches, assess the timing of when updates are made to the system, and when the most recent OFAC changes were made to the system. Also, evaluate whether all of the DD's databases are run against the automated system, and the frequency upon which searches are made. Run tests of the system by entering test account names that are the same as or similar to those recently added to the OFAC list to determine whether the system successfully identifies a potential hit for a sample of fiat-based and digital asset activity.[161]	

[161] For example, the examiner may assess the bank's approach to reviewing counterparties in a digital escrow-related contract. Such an evaluation may potentially consider how the DD is conducting fuzzy logic (e.g., to verify

Procedure	Comments
• If the DD does not use an automated system, evaluate the process used to check the existing customer base against the OFAC list and the frequency of such checks. • Pull a sample of false hits (potential matches) to check their handling; the resolution of a false hit should take place outside of the business line. • Evaluate the process related to any auto-close of alerts rules and identify whether alerts are being suppressed.	

that the name is not a strong alias to a sanctioned individual), how this information is stored or maintained, and what measures are in place to verify the accuracy of data feeds into the sanctions filtering systems.

2.4.4. OFAC Independent Testing

Objective. *Assess the DD's OFAC independent testing to evaluate whether it is appropriate for the DD's OFAC risk, taking into consideration its products, services, customers, entities, transactions, and geographic locations*.

Every DD should conduct an independent test of its OFAC compliance program that is performed by the internal audit department, outside auditors, consultants, or other qualified independent parties. For large DDs, the frequency and area of the independent test should be based on the known or perceived risk of specific business areas. For smaller DDs, the audit should be consistent with the DD's OFAC risk profile or be based on a perceived risk. The person(s) responsible for testing should conduct an objective, comprehensive evaluation of OFAC policies, procedures, and processes. The audit scope should be comprehensive enough to assess OFAC compliance risks and evaluate the adequacy of the OFAC compliance program.

Audits assess the effectiveness of current processes and check for inconsistencies between these and day-to-day operations. A comprehensive and objective testing or audit function within an SCP ensures that an organization identifies program weaknesses and deficiencies, and it is the organization's responsibility to enhance its program, including all program-related software, systems, and other technology, to remediate any identified compliance gaps. Such enhancements might include updating, improving, or recalibrating SCP elements to account for a changing risk assessment or sanctions environment. Testing and auditing can be conducted on a specific element of an SCP or at the enterprise-wide level.

General Aspects of an SCP: Testing and Auditing

A comprehensive, independent, and objective testing or audit function within an SCP ensures that entities are aware of where and how their programs are performing and should be updated, enhanced, or recalibrated to account for a changing risk assessment or sanctions environment, as appropriate. Testing or audit, whether conducted on a specific element of a compliance program or at the enterprise-wide level, are important tools to ensure the program is working as designed and to identify weaknesses and deficiencies within a compliance program. Elements of an appropriate SCP include the following:

I. The organization commits to ensuring that the testing or audit function is accountable to senior management, is independent of the audited activities and functions, and has sufficient authority, skills, expertise, resources, and authority within the organization.

II. The organization commits to ensuring that it employs testing or audit procedures appropriate to the level and sophistication of its SCP and that this function, whether deployed internally or by an external party, reflects a comprehensive and objective assessment of the organization's OFAC-related risk assessment and internal controls.

III. The organization ensures that, upon learning of a confirmed negative testing result or audit finding pertaining to its SCP, it will take immediate and effective action, to the

extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.

Further, per OFAC guidance from 2021, tests or audits—whether internal or external—should ensure that:

- Screening of the SDN List and other sanctions lists is functioning effectively and is appropriately flagging transactions for further review;
- Screening tools are appropriately flagging geographic keywords in connection with KYC-related screening or other transaction screening;
- IP address software is properly preventing users from sanctioned jurisdictions from accessing its products and services; and
- Procedures for investigating transactions identified through the screening process as having a potential sanctions nexus (e.g., transactions involving a blocked person, or a keyword related to a sanctioned jurisdiction) and procedures for blocked property or rejected transaction reporting to OFAC are reviewed.[162]

[162] OFAC, "Sanctions Compliance Guidance for Virtual Currency Industry" (October 2021).

2.4.4.1. OFAC Independent Testing – Examination Procedures

Objective. *Assess the DD's OFAC independent testing to evaluate whether it is appropriate for the DD's OFAC risk, taking into consideration its products, services, customers, entities, transactions, and geographic locations*.

Procedure	Comments
1. Determine the adequacy of independent testing (audit) and follow-up procedures.	
2. Determine whether the testing or audit function is accountable to senior management, is independent of the audited activities and functions, and has sufficient authority, skills, expertise, resources, and authority within the organization. Determine whether the DD also has a compliance monitoring and testing function responsible for conducting reviews or key OFAC compliance controls; if yes, evaluate the scope and frequency of such reviews.	
3. Determine whether the DD employs testing or audit procedures appropriate to the level and sophistication of its SCP and that this function, whether deployed internally or by an external party, reflects a comprehensive and objective assessment of the organization's OFAC-related risk assessment and internal controls. This includes evaluating the frequency and scope of tests/audits (e.g., the effectiveness of screening tools, IP address software, procedures for investigating transactions identified through the screening process as having a potential sanctions nexus, procedures for blocked property or rejected transaction reporting to OFAC).	
4. Determine whether the DD ensures that, upon learning of a confirmed negative testing result or audit finding pertaining to its SCP, takes immediate and effective action, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.	

2.4.5. OFAC Training

Objective. *Assess the DD's OFAC training to evaluate whether it is appropriate for the DD's OFAC risk, taking into consideration its products, services, customers, entities, transactions, and geographic locations*.

The DD should provide adequate training for all appropriate employees on its OFAC compliance program, procedures, and processes. The scope and frequency of the training should be consistent with the DD's OFAC risk profile and appropriate to employee responsibilities.

An effective training program is an integral component of a successful SCP. The training program should be provided to all appropriate employees and personnel on a periodic basis (and at a minimum, annually) and generally should accomplish the following: (i) provide job-specific knowledge based on need; (ii) communicate the sanctions compliance responsibilities for each employee; and (iii) hold employees accountable for sanctions compliance training through assessments.

General Aspects of an SCP: Training

An adequate training program, tailored to an entity's risk profile and all appropriate employees and stakeholders, is critical to the success of an SCP. Elements of an appropriate SCP include the following:

I. The organization commits to provide training that covers OFAC regulatory requirements, supervisory guidance, and the DD's internal OFAC policies, procedures, and processes.

II. The organization commits to ensuring that its OFAC-related training program provides adequate information and instruction to employees and, as appropriate, stakeholders (for example, clients, suppliers, business partners, and counterparties as well as any other counterparties specific to DD activity such as other exchanges or partners within a stablecoin network[163]) in order to support the organization's OFAC compliance efforts. Such training should be further tailored to high-risk employees within the organization.

III. The organization commits to provide OFAC-related training with a scope that is appropriate for the products and services it offers; the customers, clients, and partner relationships it maintains; and the geographic regions in which it operates.

IV. The organization commits to providing OFAC-related training with a frequency that is appropriate based on its OFAC risk assessment and risk profile.

V. The organization commits to ensuring that OFAC-related training is kept up to date and is updated on an ongoing basis to account for the for the evolving digital assets

[163] In this context, "counterparties" refer to the other parties involved in a transaction.

environment, including new sanctions evasion typologies and trends employed by illicit actors (e.g., the use of mixers & tumblers, AECs, DEXs/P2P exchanges with few OFAC controls, chain-hopping, darknet marketplace, the deliberate misuse of legal entities and arrangements for facilitating sanctions evasion, and high-risk geographies for ransomware and other crimes).

VI. The organization commits to ensuring that the scope of OFAC-related training includes OFAC reporting requirements, associated timelines, and recordkeeping processes, including the need to submit blocking reports to OFAC in addition to filing SARs with FinCEN in certain cases,[164] as well as initial blocked property reports, annual blocked property reporting, rejected transaction reports, on demand reports.[165]

VII. The organization commits to ensuring that, upon learning of a confirmed negative testing result or audit finding, or other deficiency pertaining to its SCP, it will take immediate and effective action to provide training to or other corrective action with respect to relevant personnel.

VIII. The organization's training program includes easily accessible resources and materials that are available to all applicable personnel.

[164] OFAC, "Sanctions Compliance Guidance for Virtual Currency Industry" (October 2021).

[165] Ibid

2.4.5.1. OFAC Training– Examination Procedures

Objective. *Assess the DD's OFAC training to evaluate whether it is appropriate for the DD's OFAC risk, taking into consideration its products, services, customers, entities, transactions, and geographic locations*.

Procedure	Comments
1. Determine whether all personnel whose duties require knowledge of OFAC are included in the training program, that OFAC compliance staff have received periodic training that is relevant and appropriate, and that the board of directors and senior management receive appropriate training that may include changes or new developments related to OFAC compliance.	
2. Determine whether the DD's OFAC training program materials address: • The importance that the board of directors and senior management place on ongoing education, training, employee accountability, and compliance. • Results of previous findings of noncompliance with internal policies and regulatory requirements, if applicable. • An overview of the purposes of OFAC and its regulatory requirements and timelines, recordkeeping requirements, supervisory guidance, and the DD's internal policies, procedures, and processes. • Information tailored to specific risks of individual business lines or operational units. • Different forms of sanctions evasion and other illicit financial activity risks as they relate to identification and examples of suspicious activity. This includes recent typologies or trends used by illicit actors (e.g., ransomware payments, the deliberate misuse of legal entities and arrangements, such as trust, for money laundering and other financial crimes) and red flags for employees to identify and appropriately escalate such activity.	

Procedure	Comments
• Information on current developments and changes to OFAC regulatory requirements, as well as relevant recent regulatory and/or industry guidance (e.g., best practices, lessons learned). • Information on relevant industry developments in the evolving digital assets landscape. • Adequate training for any agents who are responsible for conducting OFAC-related functions on behalf of the DD.	
3. Determine whether the DD maintains documentation of the dates of training sessions and training and testing materials (if testing is used by the DD). Documentation should include attendance records and any failures of personnel to take the requisite training in a timely manner, as well as any corrective actions taken to address such failures.	
4. Determine whether the DD has developed governance documentation for OFAC-related training (e.g., training policy, training needs assessment, annual training plan).	
5. Determine whether any OFAC-related training is outsourced to a third party (e.g., the use of a vendor for training material and/or delivery). To the extent third parties are used, evaluate whether the DD has a formal governance process (e.g., including the review of such training content before it is delivered to DD employees).	

2.5. Developing Conclusions and Finalizing the Exam

2.5.1. Developing Conclusions and Finalizing the Exam

Objective. *Formulate conclusions about the adequacy of the DD's AML/CFT and OFAC compliance program, relative to its risk profile, and the DD's compliance with BSA and OFAC regulatory requirements; develop an appropriate supervisory response; and communicate AML/CFT and OFAC examination findings to the DD.*

In the final phase of the AML/CFT and OFAC examination, examiners should assemble all findings from the examination and testing procedures completed. From those findings, examiners should develop and document conclusions about the adequacy of the DD's AML/CFT and OFAC compliance program, relative to its risk profile, and the DD's compliance with BSA and OFAC regulatory requirements. When formulating conclusions, examiners are reminded that DDs have flexibility in the design of their AML/CFT and OFAC compliance programs, which will vary based on the DD's risk profile, size or complexity, and organizational structure. Examiners should primarily focus on whether the DD has established appropriate processes to manage sanctions risk, ML/TF, and other illicit financial activity risks, and that the DD has complied with BSA and OFAC requirements.

Examiners should discuss with the DD their preliminary conclusions, which may include strengths, weaknesses, any deficiencies or violations, if applicable, and necessary remediation of any deficiencies or violations. Minor weaknesses, deficiencies, and technical violations alone are not indicative of an inadequate AML/CFT and/or OFAC compliance program and should not be communicated as such. Conclusions regarding the adequacy of the DD's AML/CFT and OFAC compliance programs and any significant findings should be presented in a written format for inclusion in the report of examination (ROE).[166]

In formulating a written conclusion for the ROE, examiners do not need to discuss every procedure performed during the examination. Written comments should convey to the reader whether the overall AML/CFT and OFAC compliance programs are adequate. The comments should cover areas or subjects pertinent to examiner findings and conclusions. Examiners should prepare workpapers in sufficient detail to support discussions in the ROE. To the extent items are discussed in the workpapers but not the ROE, the workpapers should appropriately document each item, as well as any other aspect of the DD's AML/CFT and OFAC compliance programs that merits attention but may not rise to the level of findings included in the ROE. Examiners should organize and reference workpapers and document conclusions and supporting information within internal agency systems, as appropriate.

Examiners should determine and document what supervisory response, if any, is recommended. The AML/CFT and OFAC examination findings may include violations of laws or regulations or

[166] ROE may include other formal supervisory correspondence, such as Supervisory Letters.

other deficiencies. Any substantive deficiencies in the AML/CFT and/or OFAC compliance programs, including violations, should be included in the ROE in such a manner that allows the reader to understand the cause of the deficiencies. The extent to which violations and other deficiencies affect the examiner's evaluation of the adequacy of the DD's AML/CFT and OFAC compliance programs and the DD's compliance with BSA and OFAC regulatory requirements is based on the nature, duration, and severity of the problem(s). In some cases, the appropriate supervisory response is for the DD to correct the violations or other deficiencies as part of the normal supervisory process. These remediation efforts should be documented in the ROE. In appropriate circumstances, however, an agency may take either informal or formal enforcement actions to address violations of BSA regulatory requirements.[167]

Violations or deficiencies can be caused by a number of issues including, but not limited to, the following:

- Management has not appropriately assessed the DD's ML/TF and other illicit financial activity risks.
- Management has not created or enhanced policies, procedures, and processes.
- Management or employees disregard, are unaware of, or misunderstand regulatory requirements or internal policies, procedures, or processes.
- Management has not adjusted the AML/CFT and/or OFAC compliance programs commensurate with growth in higher-risk operations (products, services, customers, distribution channels, and geographic locations).
- Management has not provided sufficient staffing for the DD's risk profile.
- Management has not appropriately communicated changes in internal policies, procedures, and processes.

Systemic or Repeat Violations

Systemic or repeat violations involve either a substantive deficiency or a repeated failure to comply with BSA regulatory requirements, including the requirement to establish and maintain a reasonably designed AML/CFT and OFAC compliance program. A substantive deficiency or repeated failure to comply with BSA and OFAC regulatory requirements could negatively affect the DD's ability to manage ML/TF and other illicit financial activity risks. Systemic violations are the result of substantively deficient systems or processes that fail to obtain, analyze, or maintain required information, or to report customers, accounts, or transactions, as required under various provisions of the BSA and OFAC regulations. Repeat violations are repetitive occurrences of the same or similar issues.

When evaluating whether deficiencies constitute systemic or repeat violations, examiners must analyze the pertinent facts and the totality of circumstances, including whether the deficiencies are

[167] The "Joint Statement on Enforcement Of Bank Secrecy Act/ Anti-Money Laundering Requirements" (August 2020) explains the basis for the federal banking agencies' enforcement of specific requirements of the BSA.

frequently recurring, regular, or usual, and whether the deficiencies are of the same or similar nature.

Considerations in determining whether a violation is systemic include, but are not limited to:

- Whether the number of violations is high when compared to the DD's total activity. This evaluation usually is determined through a sampling of transactions or records. Based on this process, determinations are made concerning the overall level of noncompliance. However, even if the violations are few in number, they could reflect systemic noncompliance, depending on the severity (e.g., significant or egregious).
- Whether there is evidence of similar violations by the DD in a series of transactions or in different divisions or departments. This is not an exact calculation and examiners should consider the number, significance, and frequency of violations identified throughout the organization. Violations identified within various divisions or departments may or may not indicate a systemic violation. These violations should be evaluated in a broader context to determine if training or other compliance system weaknesses are also present.
- The relationship of the violations to one another (e.g., whether the violations occurred in the same area of the DD, in the same product line, in the same branch or department, or with one employee).
- The impact the violation or violations have on the DD's suspicious activity monitoring and reporting capabilities.
- Whether the violations appear to be grounded in a written or unwritten policy or established procedure, or result from a lack of an established procedure (e.g., the DD's currency transaction reporting thresholds are inconsistent with BSA regulations).
- Whether there is a common source or cause of the violations.
- Whether the violations were the result of errors in software programming or implementation.

Systemic or repeat violations of the BSA or other deficiencies could have a negative impact on the adequacy of the DD's AML/CFT and/or OFAC compliance program.[168] When systemic instances of noncompliance are identified, examiners should consider the noncompliance in the context of the overall program (internal controls, independent testing, designated individual or individuals, and training) and refer to the Joint Statement On Enforcement Of Bank Secrecy Act/ Anti-Money Laundering Requirements[169] for more information regarding when a DD's AML/CFT compliance program may be deficient as a result of systemic noncompliance. All systemic violations and substantive deficiencies should be brought to the attention of the DD's board of directors and

[168] The violations or deficiencies may also constitute unsafe or unsound banking practices. See 12 CFR Part 30 (OCC).

[169] Board of Governors of the Federal Reserve System, FDIC, NCUA, OCC, "Joint Statement on Enforcement Of Bank Secrecy Act/ Anti-Money Laundering Requirements" (August 2020).

senior management and documented in the ROE or other supervisory correspondence directed to the board of directors.

Types of systemic or repeat violations may include, but are not limited to:

- Failure to establish a due diligence program that includes a risk-based approach, and when necessary, enhanced policies, procedures, and controls concerning foreign correspondent accounts.
- Failure to maintain a reasonably designed due diligence program for private banking accounts for non-U.S. persons (as defined in 31 CFR 1010.620).
- Frequent, consistent, or recurring late CTR or SAR filings.
- A significant number of CTRs or SARs with errors or omissions of data elements.
- Consistently failing to obtain or verify required customer identification information at account opening.
- Consistently failing to complete searches on 314(a) information requests.
- Failure to consistently maintain or retain records required by the BSA.

Also, the Joint Statement On Enforcement Of Bank Secrecy Act/ Anti-Money Laundering Requirements provides that "[t]he Agencies will cite a violation of the SAR regulations, and will take appropriate supervisory actions, if the institution's failure to file a SAR (or SARs) evidences a systemic breakdown in its policies, procedures, or processes to identify and research suspicious activity, involves a pattern or practice of noncompliance with the filing requirement, or represents a significant or egregious situation."[170]

Isolated or Technical Violations

Isolated or technical violations are limited instances of noncompliance with the BSA that occur within an otherwise adequate system of policies, procedures, and processes. These violations generally do not prompt serious regulatory concern or reflect negatively on management's supervision or commitment to BSA compliance, unless the isolated violation represents a significant or egregious situation or is accompanied by evidence of bad faith. Corrective action for isolated or technical violations is usually undertaken by the DD within the normal course of business.

Multiple isolated or technical violations throughout DD departments or divisions can indicate systemic or repeat violations. Examiners should consider multiple isolated or technical violations in the context of all examination findings, oversight provided by the DD's board of directors and senior management, and the DD's risk profile.

---

[170] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, "Joint Statement on Enforcement Of Bank Secrecy Act/ Anti-Money Laundering Requirements" (August 2020).

Types of isolated or technical violations may include, but are not limited to:

- Failure to file or late filing of CTRs that is infrequent, not consistent, or nonrecurring.
- Failure to obtain complete customer identification information for a monetary instrument sales transaction that is isolated and infrequent.
- Infrequent, not consistent, or nonrecurring incomplete or inaccurate information in SAR data fields.
- Failure to obtain or verify required customer identification information that is infrequent, not consistent, or nonrecurring.
- Failure to complete a 314(a) information request that is inadvertent or nonrecurring.

2.5.1.1. Developing Conclusions and Finalizing the Examination Procedures

Objective. *Formulate conclusions about the adequacy of the DD's AML/CFT compliance program, relative to its risk profile, and the DD's compliance with BSA regulatory requirements; develop an appropriate supervisory response; and communicate AML/CFT examination findings to the DD.*

Procedure	Comments
AML/CFT Conclusions	
1. Accumulate all pertinent findings from the AML/CFT examination and testing procedures performed.	
2. Formulate conclusions about the adequacy of the DD's AML/CFT compliance program. Prepare written comments for the ROE covering areas or subjects pertinent to findings and conclusions. Prepare workpapers in sufficient detail to support discussions in the ROE. Reach a preliminary conclusion as to whether: • The DD understands its ML/TF and other illicit financial activity risks. This may be determined by reviewing the DD's risk assessment process, including whether the risk assessment provides a comprehensive analysis of the ML/TF and other illicit financial activity risks of the DD and is provided to all business lines across the DD, the board of directors, management, and appropriate staff. • The AML/CFT compliance program is written, approved by the board of directors, and noted in the board minutes. • AML/CFT policies, procedures, and processes are reasonably designed to assure and monitor compliance with the BSA and appropriately address higher-risk operations (products, services,	

Procedure	Comments
customers, transactions, distribution channels, and geographic locations). The DD's practices correspond to the policies, procedures, and processes. • Internal controls are reasonably designed to manage the DD's ML/TF and other illicit financial activity risks and to assure compliance with the BSA, especially for higher-risk operations (products, services, customers, and geographic locations). • Independent testing (audit) is adequate to assess the DD's compliance with BSA regulatory requirements and assess the overall adequacy of the AML/CFT compliance program. The overall independent testing coverage and frequency are appropriate in relation to the ML/TF and other illicit financial activity risk profile of the DD, as well as any expansionary activity. Transaction testing performed is adequate, particularly for higher-risk banking operations and suspicious activity monitoring systems. • The designated individual or individuals responsible for coordinating and monitoring day-to-day compliance is competent, has properly executed policies and procedures, and has the appropriate authority, independence, and access to resources. • Personnel are sufficiently trained to follow legal, regulatory, and policy requirements. • The board of directors and senior management are aware of AML/CFT regulatory requirements, adequately oversee AML/CFT compliance, and commit, as necessary, to corrective actions that address independent testing	

Procedure	Comments
or regulatory examination findings and recommendations in a timely manner. The board of directors and senior management clearly communicate the need and support for AML/CFT risk management and internal controls throughout the organization. • Communication of policies, procedures, and processes is adequate throughout the DD. • The AML/CFT compliance program is reasonably designed to assure and monitor compliance with the BSA relative to the DD's overall ML/TF and other illicit financial activity risks.	
3. Prepare written comments for the ROE documenting any deficiencies or violations identified. Prepare written comments for workpapers regarding any supervisory response that may be appropriate. The written comments should discuss the nature, duration, and severity of the deficiencies or violations and the necessary remediation by the DD. Note whether deficiencies or violations were previously identified by the DD or independent testing, or were only identified as a result of an examination.	
4. Discuss preliminary findings with the examiner-in-charge or the examiner responsible for the AML/CFT examination. Specifically, discuss any findings that have been or will be discussed with the DD, such as: • A conclusion regarding the adequacy of the DD's AML/CFT compliance program and the DD's compliance with BSA regulatory requirements. • Any identified deficiencies or violations, and an assessment of the severity of the issues.	

Procedure	Comments
• Actions needed by the DD to correct violations or deficiencies. • Preliminary recommendations for a supervisory response, if necessary. ○ If the agency may need to take either an informal or formal enforcement action to address violations of BSA regulatory requirements, examiners should discuss this fact with appropriate agency supervision management and legal staff.	
OFAC Conclusions	
5. Identify whether there are any deficiencies in the OFAC compliance program, then determine the origin of any deficiencies (e.g., training, audit, risk assessment, internal controls, management oversight), and conclude on the adequacy of the DD's OFAC compliance program.	
6. Identify any potential matches that were not reported to OFAC, discuss with DD management, advise DD management to immediately notify OFAC of unreported transactions, and immediately notify supervisory personnel at your regulatory agency.	
7. Discuss OFAC related examination findings with DD management.	
8. Include OFAC conclusions within the report of examination, as appropriate.	
Overall Conclusions	
9. Based on the overall assessment, provide overall findings based on the DD's overall AML/CFT and OFAC Compliance Program.	

3. ASSESSING COMPLIANCE WITH BSA REGULATORY REQUIREMENTS

3.1. Customer Identification Program

Objective. *Assess the DD's compliance with the BSA regulatory requirements for the Customer Identification Program (CIP).*

Regulatory Requirements for Customer Identification Programs

This section outlines the regulatory requirements for DDs in 12 CFR Chapters I through III and VII, and 31 CFR Chapter X regarding CIPs. Specifically, this section covers:

- 12 CFR 21.21(c)(2)
- 12 CFR 208.63(b)(2), 12 CFR 211.5(m)(2), 12 CFR 211.24(j)(2)
- 12 CFR 326.8(b)(2)
- 12 CFR 748.2(b)(2)
- 31 CFR 1020.220

A DD must have a written CIP that is appropriate for its size and type of business and that includes certain minimum requirements. The CIP must be incorporated into the DD's AML/CFT compliance program, which is subject to approval by the DD's board of directors. Minor weaknesses, deficiencies, and technical violations alone are not indicative of an inadequate CIP.

Identity Verification Procedures

The CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. The procedures must enable the DD to form a reasonable belief that it knows the true identity of each customer and be based on the DD's assessment of relevant risks, including:

- The types of accounts maintained by the DD.
- The DD's methods of opening accounts.
- The types of identifying information available.
- The DD's size, location, and customer base.

For purposes of the CIP rule, an "account" is a formal banking relationship established to provide or engage in services, dealings, or other financial transactions, including a deposit account, a transaction or asset account, a credit account, or other extension of credit. An account includes a relationship established to provide a safety deposit box or other safekeeping services, or cash management, custodian, and trust services.

An account does not include:

- A product or service where a formal banking relationship is not established with a person, such as check-cashing, wire transfer, or sale of a check or money order;
- An account that the DD acquires through an acquisition, merger, purchase of assets, or assumption of liabilities; or
- An account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974.

The CIP rule applies to a customer, which means:

- A person that opens a new account; and
- An individual who opens a new account for:
    - An individual who lacks legal capacity, such as a minor; or
    - An entity that is not a legal person, such as a civic club.

A customer does not include a person who does not receive banking services, such as a person whose loan application is denied or a person that has an existing account with the DD, provided that the DD has a reasonable belief that it knows the true identity of the person. Also excluded from the definition of customer are financial institutions regulated by a federal functional regulator or a DD regulated by a state DD regulator, governmental entities, and publicly traded companies as described in 31 CFR 1020.315(b)(2) through (b)(4).

Customer Information Required

The CIP must contain account-opening procedures detailing the identifying information to obtain from each customer. At a minimum, the DD must obtain the following identifying information from each customer before opening the account:

- Name,
- Date of birth for an individual,
- Address, and
- Identification number.

The CIP rule provides for an exception for opening an account for a customer who has applied for a tax identification number (TIN).

- The exception permits the DD to open an account for a customer who has applied for a TIN, but does not yet have a TIN. In this case, the DD's CIP must include procedures to confirm that the application was filed before the customer opens the account and to obtain the TIN within a reasonable period of time after the account is opened.

Based on its AML/CFT risk assessment, a DD may require identifying information, in addition to the required information, for certain customers or product lines.

Customer Verification

The CIP must contain risk-based procedures for verifying the identity of the customer within a reasonable period of time after the account is opened. The verification procedures must use the "information obtained in accordance with [31 CFR 1020.220(a)(2)(i)]," namely the identifying information obtained by the DD. A DD need not establish the accuracy of every element of identifying information obtained, but it must verify enough information to form a reasonable belief that it knows the true identity of the customer. The DD's procedures must describe when it uses documents, non-documentary methods, or a combination of both methods to verify the identity of its customers, as well as when it uses electronic verification to verify a customer's identity. It is particularly important for DDs to ensure they have robust, comprehensive, and reliable identity verification tools/solutions that accord with their risk appetite.[171] DDs may be required to employ a layered approach of multiple capabilities (or tools/solutions) to fully discharge their AML/ATF responsibilities at scale. It is considered a best practice for DDs to find a single, easy-to-use API that seamlessly integrates into the DD's broader system and infrastructure. DDs are encouraged to leverage identity verification tools that use machine learning, AI, facial biometrics, information scoring tools, knowledge-based authentication, photographs, voice verification, and videos (i.e., liveness detection).

Verification Through Documents

A DD relying on documents to verify a customer's identity must have procedures that set forth the documents that the DD will use. The CIP rule gives examples of the types of documents that may be used to verify a customer's identity. The rule reflects the federal banking agencies' expectations that, for most customers who are individuals, DDs review an unexpired government-issued form of identification evidencing a customer's nationality or residence and bearing a photograph or similar safeguard; examples include a driver's license or passport. However, other forms of identification may be used if they enable the DD to form a reasonable belief that it knows the true identity of the customer. Given the availability of counterfeit and fraudulently obtained documents, a DD is encouraged to review more than a single document to ensure it can form a reasonable belief that it knows the true identity of the customer, particularly where customers are being onboarded through solely electronic means in a non-face-to-face context, as is often the case with DDs.

For a person other than an individual (such as a corporation, partnership, or trust), documents may include those showing the legal existence of the entity, such as certified articles of incorporation, an unexpired government-issued business license, a partnership agreement, or a trust instrument.

[171] FATF, "Guidance on Digital Identity" (March 2020).

Verification Through Non-Documentary Methods

A DD using non-documentary methods to verify a customer's identity must have procedures that set forth the methods the DD uses (e.g., electronic data proofing, open-source intelligence, EIN verification, recognized third-party databases, public registries, etc.). Non-documentary methods may include contacting a customer; independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement.

If the DD uses non-documentary methods to verify a customer's identity, the DD's procedures must address situations in which an individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard; the DD is not familiar with the documents presented; the account is opened without obtaining documents; the customer opens the account without appearing in person at the DD; and where the DD is otherwise presented with circumstances that increase the risk that the DD will be unable to verify the true identity of a customer through documents.

Additional Verification for Certain Customers

The CIP must address situations in which, based on its risk assessment of a new account opened by a customer that is not an individual, the DD will obtain information about individuals with authority or control over such account, including signatories, in order to verify the customer's identity. This verification method applies only when the DD cannot verify the customer's true identity using documents or non-documentary methods.

Lack of Verification

The CIP must also have procedures for responding to circumstances in which the DD cannot form a reasonable belief that it knows the true identity of the customer. These procedures should describe:

- When the DD should not open an account;
- The terms under which a customer may use an account while the DD attempts to verify the customer's identity;
- When the DD should close an account, after attempts to verify a customer's identity have failed; and
- When the DD should file a suspicious activity report (SAR) in accordance with applicable law and regulation.

Recordkeeping and Retention Requirements

The DD's CIP must include procedures for making and maintaining a record of all information obtained to identify and verify a customer's identity. At a minimum, the DD must retain all identifying information (name, date of birth for an individual, address, identification number, and any other identifying information obtained under 31 CFR 1020.220(a)(2)(i)) at account opening for CIP purposes for a period of five years after the account is closed.

A DD may keep copies of identifying documents that it uses to verify a customer's identity; however, the CIP rule does not require it. A DD's verification procedures must be risk-based and, in certain situations, keeping copies of identifying documents may be warranted. In addition, a DD may have procedures to keep copies of the documents for other purposes, for example, to facilitate investigating potential fraud. If the DD retains copies of identifying documents in lieu of a description, these documents must be retained in accordance with the general recordkeeping requirements in 31 CFR 1010.430, "Nature of Records and Retention Period." Nonetheless, a DD should not improperly use any document containing a picture of an individual, such as a driver's license, in connection with any aspect of a credit transaction.

The DD must also keep a description of the following for five years after the record is made:

- Any document that was relied on to verify identity, noting the type of document, any identification number contained in the document, the place of issuance, and, if any, the date of issuance and expiration date;
- The methods and the results of any measures undertaken to verify the identity of the customer using non-documentary methods or additional verification procedures for certain customers; and
- The resolution of any substantive discrepancy discovered when verifying the identifying information obtained.

Comparison with Government Lists

The CIP must include procedures for determining whether the customer appears on any list of known or suspected terrorists or terrorist organizations issued by any federal government agency and designated as such by Treasury in consultation with the federal functional regulators. The procedures must require the DD to make such a determination within a reasonable period of time after the account is opened, or earlier, if required by another federal law or regulation or federal directive issued in connection with the applicable list. The procedures must also require the DD to follow all federal directives issued in connection with such lists. DDs will receive notification by way of separate guidance regarding the list that must be consulted for purposes of this provision.

As of the publication date of this Manual, no designated government lists for CIP purposes exist. Checking of customers against Office of Foreign Assets Control (OFAC) lists and 31 CFR 1010.520 (commonly referred to as section 314(a) requests) remain separate and distinct requirements.

Adequate Customer Notice

The CIP must include procedures for providing DD customers with adequate notice that the DD is requesting information to verify their identities. Notice is adequate if the DD generally describes the identification requirements of the CIP rule and provides the notice in a manner reasonably designed to ensure that a customer is able to view or otherwise receive the notice before the account is opened. Depending on the manner in which an account is opened, examples of adequate notice may include posting a notice in the lobby or on the DD's website, including a notice with account application documents, or providing other written or oral notice. The sample language below is provided in the regulation:

Important Information About Procedures for Opening a New Account

To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.

What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

Reliance on Another Financial Institution

The DD's CIP may include procedures specifying when a DD will rely on the performance by another financial institution (including an affiliate) of any procedures of the DD's CIP with respect to any customer of the DD that is opening, or has opened, an account or has established a similar formal banking or business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions, provided that:

- Such reliance is reasonable under the circumstances;
- The other, relied-upon financial institution is subject to a rule implementing 31 USC 5318(h) and is regulated by a federal functional regulator; and
- The other financial institution enters into a contract requiring it to certify annually to the DD that it has implemented its AML program, and that it will perform (or its agent will perform) the specified requirements of the DD's CIP.

Exemptions

The appropriate federal functional regulator, with the concurrence of FinCEN on behalf of the Secretary of the Treasury, may, by order or regulation, exempt any DD or type of account from the requirements of this section. The federal banking agencies, with FinCEN's concurrence, have granted a CIP exemption for loans extended by DDs and their subsidiaries to all customers to facilitate purchases of property and casualty insurance policies (referred to as premium finance

loans). The federal banking agencies found that the exemption is consistent with the purposes of the BSA, based on FinCEN's determination that premium finance loans present a low risk of money laundering or terrorist financing (ML/TF), and that this exemption is consistent with safe and sound banking.

Other Legal Requirements

Nothing in the CIP rule relieves a DD of its obligation to comply with any other provision of the BSA, including provisions concerning information that must be obtained, verified, or maintained in connection with any account or transaction.

Use of Third Parties

The CIP rule does not alter a DD's authority to use a third party, such as an agent or service provider, to perform services on its behalf. Therefore, a DD may arrange for a third party, acting as its agent in connection with a transaction, to verify the identity of its customer. For example, a DD's customer may use a third-party digital assets exchange to obtain cryptocurrency that ultimately lands in his or her DD wallet, and the DD may utilize the services of the third-party digital assets exchange to verify the identity of the customer. The DD can also arrange for a third party to maintain its records. However, as with other responsibilities performed by a third party, the DD is ultimately responsible for compliance with the requirements of the CIP rule. Examiners should refer to their agency's relevant guidance and requirements for such third-party relationships.

Additional Resources

The U.S. Department of the Treasury, FinCEN, and the federal banking agencies have issued Frequently Asked Questions (FAQs), which may be revised periodically. FinCEN and the federal banking agencies have issued interagency guidance on applying CIP requirements to holders of prepaid cards. There is also guidance encouraging the use of non-documentary verification methods permitted by the CIP requirements for customers who cannot provide standard identification documents because of the effects of natural disasters. The FAQs, guidance, exceptive relief, and other related documents (e.g., the CIP rule) are available on the websites of FinCEN and the federal banking agencies.

Examiner Assessment of the CIP Process

Examiners should assess the adequacy of the DD's policies, procedures, and processes (internal controls) related to the DD's CIP. Specifically, examiners should determine whether these internal controls are designed to mitigate and manage ML/TF and other illicit financial activity risks and comply with CIP requirements. Examiners may review other information, such as recent independent testing or audit reports, to aid in their assessment of the DD's CIP.

Examiners should also consider general internal controls concepts, such as dual controls, segregation of duties, and management approval for certain actions, as they relate to the DD's CIP. Other internal controls may include BSA compliance officer or other senior management approval for staff actions that deviate from the DD's CIP policies, procedures, and processes. Additionally, examiners should evaluate the tools and/or solutions employed by the DD for conducting identity verification (e.g., the use of machine learning, AI, facial biometrics, etc.), including the controls the DD has established around such tools and/or solutions to determine their independence, accuracy, and reliability.[172] When assessing internal controls and CIP compliance, examiners should keep in mind that the DD may have limited instances of noncompliance with the CIP rule (such as isolated or technical violations) or minor deviations from the DD's CIP policies, procedures, and processes without resulting in an inadequate CIP.

Examiners should determine whether the DD's internal controls for CIP are designed to assure ongoing compliance with the requirements and are commensurate with the DD's size or complexity and organizational structure. More information can be found in the *Assessing the AML/CFT Compliance Program - AML/CFT Internal Controls* section of this Manual.

[172] Examiners may look to FATF's Guidance on Digital Identity which states: "[T]he requirement that digital "source documents, data or information" must be "reliable, independent" means that the digital ID system used to conduct CDD relies upon technology, adequate governance, processes and procedures that provide appropriate level of confidence that the system produces accurate results." (March 2020).

3.1.1. Customer Identification Program Examination and Testing Procedures

Objective. *Assess the DD's compliance with the BSA regulatory requirements for the Customer Identification Program (CIP).*

Procedure	Comments
1. Verify that the DD has a written CIP appropriate for its size and type of business. The written program must be included within the DD's AML/CFT compliance program and must contain procedures that address: • Obtaining the required identifying information (including name, date of birth for an individual, address, and identification number). • Verifying the identity of each customer to the extent reasonable and practicable through risk-based procedures (e.g., documentary, non-documentary, and electronic verification methods). • Responding to circumstances in which the DD cannot form a reasonable belief that it knows the true identity of a customer, including determining when a suspicious activity report (SAR) should be filed. • Complying with recordkeeping requirements. • Timely checking of new accounts against prescribed government lists, if applicable. • Providing adequate customer notice. • Relying on another financial institution that has an AML compliance program and is regulated by a federal functional regulator, if applicable.	

Procedure	Comments
2. Verify that the DD establishes appropriate controls and review procedures for its relationships with third parties, if applicable. If the DD is using a third party, such as an agent or service provider, to perform elements of its CIP, determine whether the DD has procedures in place to monitor for and ensure adequate performance. Where the DD relies on a technology solution or system to support its CIP program, determine that the DD has put in place processes to assess the reliability and independence of such technology solution or system, including whether the solution or system has in place adequate governance, processes and procedures that provide appropriate level of confidence that the solution or system produces accurate results.	
3. Determine whether the DD's CIP appropriately considers the types of accounts maintained; methods of account opening; the types of identifying information available; and the DD's size, location, and customer base.	
4. Select a sample of new accounts opened since the most recent examination to review for compliance with the DD's CIP. The sample should include a cross-section of accounts as indicated by the DD's risk assessment (e.g., consumers and businesses, loans and deposits, and accounts opened via U.S. mail and online). The sample should also, on a risk basis, include the following: • New accounts opened using the exception for customers that have applied for a TIN.	

Procedure	Comments
• New accounts opened using documentary methods, and new accounts opened using non-documentary methods. • New accounts identified by the DD as higher risk. • New accounts opened with incomplete verification information, if applicable. • New accounts opened by a third party as the DD's agent (e.g., indirect loans), if applicable.	
5. From the previous sample of new accounts, determine whether the DD has performed the following procedures: • Opened the account in accordance with the DD's policies, procedures, and processes for CIP. • Obtained from each customer, before opening the account, the identifying information required by the CIP: name, date of birth (for an individual), address, and identification number. • Verified the identity of the customer at account opening, or within a reasonable time after account opening, to the extent reasonable and practicable. • Appropriately resolved situations in which customer identity could not be reasonably verified and filed SARs, as appropriate. • Made and maintained a record of the identifying information required by the CIP regulations; a description of any document that was relied upon to verify identity; the methods and results of any measures undertaken to verify identity using non-documentary methods or	

Procedure	Comments
additional verification procedures; and verification results (including results of substantive discrepancies). • Compared the customer's name against any list of known or suspected terrorists or terrorist organizations, if applicable.	
6. Review the adequacy of the DD's customer notice and the timing of the notice's delivery.	
7. If the DD relies on other financial institutions to perform its CIP (or portions of its CIP), select a sample of new accounts opened under the reliance provision. • Determine whether the DD's customer is opening or has opened an account at, or has established a similar formal banking or business relationship with, the other financial institution to provide or engage in services, dealings, or other financial transactions. • Determine whether the other financial institution is subject to a final rule implementing the AML program requirements of 31 USC 5318(h) and is regulated by a federal functional regulator. • Review the contract between the parties, annual certifications, and other information, such as the other financial institution's CIP. • Determine whether reliance is reasonable. The contract and certification provide a standard means for a DD to demonstrate that it has satisfied the "reliance provision," unless the examiner has reason to believe that the DD's reliance is not	

Procedure	Comments
reasonable (e.g., the other financial institution has been subject to an enforcement action for AML or BSA deficiencies or violations).	
8. Review the internal controls in place for CIP. Determine whether the DD's internal controls are designed to assure ongoing compliance with CIP requirements and are commensurate with the DD's size or complexity and organizational structure. This includes reviewing the tools and/or solutions employed by the DD for conducting identity verification (e.g., the use of machine learning, AI, facial biometrics, etc.).	
9. Review any identified instances of noncompliance with the CIP rule and any deviations from the DD's CIP policies, procedures, and processes to determine whether the DD is effectively implementing its CIP. In making this determination, examiners should keep in mind that the DD may have limited instances of noncompliance with the CIP rule (such as isolated or technical violations) or minor deviations from the DD's CIP policies, procedures, and processes without resulting in an inadequate CIP.	
10. On the basis of examination and testing procedures completed, form a conclusion about the adequacy of policies, procedures, and processes the DD has developed to meet BSA regulatory requirements associated with CIP.	

3.2. Customer Due Diligence – Overview

Objective. *Assess the DD's compliance with the regulatory requirements for customer due diligence (CDD).*

The cornerstone of a strong AML/CFT compliance program is the adoption and implementation of risk-based CDD policies, procedures, and processes for all customers, particularly those that present a higher risk for money laundering and terrorist financing. The objective of CDD is to enable the DD to understand the nature and purpose of customer relationships, which may include understanding the types of transactions in which a customer is likely to engage. These processes assist the DD in determining when transactions are potentially suspicious. For DDs, it is particularly important to tailor customer due diligence for different digital assets customer types (e.g., individual, high net worth, and institutional customers will require different customer due diligence) in order to assess each customer based on its risk profile. Responses to questions around source of funds, coin usage, expected activity, and purpose of account will vary depending on the customer's profile. Moreover, different industries for institutional customers can be a helpful indicator for establishing the customer's risk profile and identifying deviations from expected activity (e.g., digital asset miners are likely to be depositing digital assets with the DDs while institutional hedge funds are likely to be converting fiat currency into digital assets for investment strategies).

Effective CDD policies, procedures, and processes provide the critical framework that enables the DD to comply with regulatory requirements including monitoring for and reporting of suspicious activity. An illustration of this concept is provided in Appendix K ("Customer Risk versus Due Diligence and Suspicious Activity Monitoring") of the FFIEC AML Manual. CDD policies, procedures, and processes are critical to the DD because they can aid in:

- Detecting and reporting unusual or suspicious activity that potentially exposes the DD to financial loss, increased expenses, or other risks.
- Avoiding criminal exposure from persons who use or attempt to use the DD's products and services for illicit purposes.
- Adhering to safe and sound banking practices.

Customer Due Diligence

FinCEN's final rule on CDD became effective July 11, 2016, with a compliance date of May 11, 2018. The rule codifies existing supervisory expectations and practices related to regulatory requirements and therefore, nothing in this final rule is intended to lower, reduce, or limit the due diligence expectations of the federal functional regulators or in any way limit their existing regulatory discretion.[173]

[173] Department of the Treasury, FinCEN, "Customer Due Diligence Requirements for Financial Institutions," final rules (RIN 1506-AB25), *Federal Register*, vol. 81, p. 29403 (May 2016).

In accordance with regulatory requirements, all DDs must develop and implement appropriate risk-based procedures for conducting ongoing customer due diligence,[174] including, but not limited to:

- Obtaining and analyzing sufficient customer information to understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
- Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers. Additional guidance can be found in the examination procedures "Beneficial Ownership Requirements for Legal Entity Customers" in the FFIEC AML Manual.

FinCEN provided further clarification of these principles on August 3, 2020. This guidance reinforces the risk-based basis for collecting information around customer activity, establishing customer risk profiles, and determining the frequency for updating customer information. The guidance highlights that "information collected throughout the relationship is critical in understanding the customer's transactions in order to assist the financial institution in determining when transactions are potentially suspicious."[175] The U.S. Treasury published its 2022 National Risk Assessments for ML/TF and proliferation financing and found that AML/CFT-related deficiencies primarily stem from inadequate CDD and enhanced due diligence ("EDD"), as well as insufficient customer risk identification. In particular, it highlights the importance of collecting adequate beneficial ownership information due to challenges associated with lack of timely access to beneficial ownership information of legal entities, the intentional misuse of legal entities and arrangements, including limited liability companies and other corporate vehicles, trusts, and partnerships, and the use of nominees, as well as instances where opaque legal structures, such as shell companies, are exploited by illicit actors to obfuscate the origin and ownership of funds.[176]

Similarly, on an international front, under the EU's 5th AML Directive (or "5AMLD"), registered digital asset service providers are required to have stronger customer due diligence controls around beneficial ownership, with a particular focus on the beneficial ownership of trusts and other opaque legal entity structures.[177]

Given the novel nature of DDs and their unique customer types, DDs need to be mindful that their CDD controls are appropriately tailored to the unique nature and complexities associated with their customer base, including the outsized representation of complex and opaque legal

---

[174] See 31 CFR 1020.210(b)(5).

[175] FinCEN, "Frequently Asked Questions Regarding Customer Due Diligence (CDD) Requirements for Covered Financial Institutions" (August 2020).

[176] U.S. Treasury, "National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing" (March 2022).

[177] European Commission, "5th Anti-Money Laundering Directive" (May 2018).

entity/arrangement structures (e.g., funds, trusts, corporate vehicles, family offices) associated with digital asset activity.

At a minimum, the DD must establish risk-based CDD procedures that:

- Enable the DD to understand the nature and purpose of the customer relationship in order to develop a customer risk profile.
- Enable the DD to conduct ongoing monitoring
  - for the purpose of identifying and reporting suspicious transactions and,
  - on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers.

In addition, the DD's risk-based CDD policies, procedures, and processes should:

- Be commensurate with the DD's AML/CFT risk profile, with increased focus on higher risk customers (including customers with opaque or complex legal entity/arrangement structures), and address off-balance sheet activity including the different types of activity and recordkeeping requirements associated with the customer's activity.
- Contain a clear statement of management's and staff's responsibilities, including procedures, authority, and responsibility for reviewing and approving changes to a customer's risk profile, as applicable. Considerations may also include what triggers the DD has in place to determine whether a customer warrants additional due diligence or a customer data refresh (e.g., use of a new higher-risk product or service).[178]
- Provide standards for conducting and documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.

Customer Risk Profile

The DD should have an understanding of the money laundering and terrorist financing risks of its customers, referred to in the rule as the customer risk profile.[179] This concept is also commonly referred to as the customer risk rating. Any customer account may be used for illicit purposes, including money laundering or terrorist financing. Further, a spectrum of risks may be identifiable even within the same category of customers. The DD's program for determining customer risk profiles should be sufficiently detailed to distinguish between significant variations in the money laundering and terrorist financing risks of its customers. Improper identification and assessment

[178] For example, the Department may also assess what processes the DD has in place to assess the customer's risk profile if introducing additional products and services, or if adding new beneficial owners, new wallet addresses associated with the account, new sources or destination of funds, or other considerations.

[179] See 31 CFR 1020.210(b)(5)(i).

of a customer's risk can have a cascading effect, creating deficiencies in multiple areas of internal controls and resulting in an overall weakened BSA compliance program.

The assessment of customer risk factors is DD-specific, and a conclusion regarding the customer risk profile should be based on a consideration of all pertinent customer information, including ownership information generally. Similar to the DD's overall risk assessment, there are no required risk profile categories, and the number and detail of these categorizations will vary based on the DD's size and complexity. Any one single indicator is not necessarily determinative of the existence of a lower or higher customer risk. However, given the unique nature of digital assets, Department examiners should assess DD processes to account for DD-specific products and activities, including the use of different types of digital assets for each product and service offered as part of the customer's risk profile.

Examiners should primarily focus on whether the DD has effective processes to develop customer risk profiles as part of the overall CDD program. Examiners may review individual customer risk decisions as a means to test the effectiveness of the process and CDD program. In those instances where the DD has an established and effective customer risk decision- making process, and has followed existing policies, procedures, and processes, the DD should not be criticized for individual customer risk decisions unless it impacts the effectiveness of the overall CDD program, or is accompanied by evidence of bad faith or other aggravating factors. Examiners should also evaluate whether the DD has updated its customer risk rating methodology (and model) and ensured it is incorporated into the DD's overall risk assessment. Given the novelty of the DD's activities, Department examiners should evaluate the DD's assessment criteria, and its rationale for how it determines thresholds and parameters around its approach for customer risk profiles, including receipt of any testing performed to determine risk profiles.

The DD should gather sufficient information about the customer to form an understanding of the nature and purpose of customer relationships at the time of account opening. This understanding may be based on assessments of individual customers or on categories of customers. An understanding based on "categories of customers" means that for certain lower-risk customers, the DD's understanding of the nature and purpose of a customer relationship can be developed by inherent or self-evident information such as the type of customer, the type of account opened, or the service or product offered.

The factors the DD should consider when assessing a customer risk profile are substantially similar to the risk categories considered when determining the DD's overall risk profile. The DD should identify the specific risks of the customer or category of customers, and then conduct an analysis of all pertinent information in order to develop the customer's risk profile. In determining a customer's risk profile, the DD should consider risk categories, such as the following, as they relate to the customer relationship:

- Products and Services.
- Customers and Entities.
- Transactions (including specific digital asset exposures, where relevant).
- Geographic Location(s).

- Distribution Channels.

As with the risk assessment, the DD may determine that some factors should be weighted more heavily than others. For example, certain products and services used by the customer, the type of customer's business, the geographic location where the customer does business, or the access and anonymity features of a technology used by the business to move digital assets, may pose a higher risk of money laundering or terrorist financing. Also, actual or anticipated activity in a customer's account can be a key factor in determining the customer risk profile. Certain products and services, including digital assets, pose a higher risk; accordingly, DDs should have clear processes in place to identify the types of products and services and digital assets the customer intends to use, as well as the purpose of the account and selected digital asset mix (e.g., speculative trading, settlement, remittance, etc.). Refer to the further description of identification and analysis of specific risk categories in *2.2.1. AML/CFT Risk Assessment* for additional information.

Customer Information – Risk-Based Procedures

As described above, the DD is required to form an understanding of the nature and purpose of the customer relationship. The DD may demonstrate its understanding of the customer relationship through gathering and analyzing information that substantiates the nature and purpose of the account. Customer information collected under CDD requirements for the purpose of developing a customer risk profile and ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, includes beneficial ownership information for legal entity customers. However, the collection of customer information regarding beneficial ownership is governed by the requirements specified in the beneficial ownership rule. The beneficial ownership rule requires the DD to collect beneficial ownership information at the 25 percent ownership threshold regardless of the customer's risk profile. In addition, the beneficial ownership rule does not require the DD to collect information regarding ownership or control for certain customers that are exempted or not included in the definition of legal entity customer, such as certain trusts, or certain other legal entity customers.[180]

Other than required beneficial ownership information, the level and type of customer information should be commensurate with the customer's risk profile, therefore the DD should obtain more customer information for those customers that have a higher customer risk profile and may find that less information for customers with a lower customer risk profile is sufficient. Additionally, the type of appropriate customer information will generally vary depending on the customer risk profile and other factors, for example, whether the customer is a legal entity or an individual. For lower risk customers, the DD may have an inherent understanding of the nature and purpose of the customer relationship (*i.e.,* the customer risk profile) based upon information collected at account opening. As a result, the DD may not need to collect any additional customer information for these customers in order to comply with this part of the CDD requirements.

[180] See 31 CFR 1010.230(e)(2) and 31 CFR 1010.230(h),

DDs are expected to collect additional types of customer information relevant to customers transacting in digital assets. Such additional information could include:

- an IP address with an associated time stamp;
- geo-location data;
- device identifiers;
- virtual currency wallet addresses;
- whether the customer used a VPN; and
- transaction hashes.[181]

DDs should also, however, take advantage of the immutable nature of the blockchain ledger. The blockchain ledger allows DDs a historical view of the digital asset's transfers (or "hops") between digital asset wallet addresses, allowing visibility into the transaction lineage in a way not feasible for traditional funds transfers. Although the individual or entity that owns the digital asset is not identifiable on the blockchain, absent the use of mechanisms to break the connection between a sending address and the addresses receiving a digital asset (i.e., tumbling or mixing),[182] the record of a digital asset, and its transaction history, is effectively available with the appropriate tools in place. In the case of tumbling or mixing, it is possible to ask for evidence of the entry point into tumbling, and then use this information to conduct an assessment. To address these novel circumstances, a capability in the digital asset space is the use of analytics tools to mitigate gaps in traditional AML-related controls due to the characteristics of digital assets. The Department requires DDs to employ a third-party digital asset analytics provider, or if in-house, demonstrate with third-party verification that the DD can conduct these analytics capabilities in-house. Though not an exhaustive list (and often used together), these control measures typically include:

- **Determination (or verification) of the identity of a digital asset wallet owner.** Because digital asset wallet addresses are inherently pseudonymous, DDs need tools to help identify and track the identity of the institution(s) associated with a digital asset wallet if it is a custodian or exchange, or the owner in the case of an unhosted wallet. Certain analytics providers offer solutions that allow DDs to obtain identifying information (e.g., wallet address of a specific exchange) that ties directly to the pseudonymous on-chain data on the blockchain ledger. Note, however, that these solutions typically limit wallet identification to an exchange or wallet address, but do not perform underlying customer identification, including ultimate beneficial ownership. Accordingly, DDs should have policies, processes, and procedures in place to demonstrate how they leverage such analytics solutions in order to form an overall customer profile and screen counterparty (i.e., the other party in a transaction) information as reasonably practicable.

---

[181] See Recommendation 10 guidance on page 41 of "Guidance For a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," (June 2019).

[182] FinCEN explains: "Mixing or tumbling involves the use of mechanisms to break the connection between an address sending CVC and the addresses receiving CVC." See "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 9, 2019).

- **Risk profiling of hosted and unhosted digital asset wallets.** Because digital assets can be transferred to or from non-regulated financial institutions absent controls, DDs should have policies, processes, and procedures in place to form a risk profile of the counterparties to whom the DD may have exposure. It is important to note that the digital assets industry faces limitations in identifying underlying information for unhosted wallets which may prevent a DD from being able to confirm counterparty information and limit its ability to properly form a risk profile. A DD should consider its risk appetite in allowing transactions with unhosted wallets, or unlabeled wallets (where it is not known whether a wallet address is associated with an unhosted wallet versus a hosted wallet) and establish policies, processes, and procedures to mitigate associated risks. Risk profiling, or the ability to leverage open-source and proprietary data to develop specific profiles typically with a quantitative score, should clearly define the risk for any entity with whom the DD interacts (e.g., VASPs) as well as customers of these entities. Department examiners should assess the DD's approach around criteria used to develop risk profiles and scores, if appropriate (e.g., risk profiling methodology), with appropriate testing and evidence tying that approach to the DD's own control processes (e.g., via historical SAR filings, findings from independent testing, the most recent risk assessment, or otherwise). Department examiners should also evaluate the degree to which the DD's risk profiling methodology provides a rationale for how scores are developed based on the DD's risk profile, and how the score is tied back to the DD's overall risk appetite.
- **Source of funds.** Given the higher risks associated with source and destination of funds, the Department encourages DDs to conduct a risk-focused source of funds review for each DD customer that conducts digital asset activity at onboarding and on a risk basis afterwards. Source of funds generally refers to the origin of the particular funds and/or assets relevant to the establishment of a business relationship or the undertaking of transactions without an account being opened.[183] DDs should leverage insights from distributed ledger analytics to assist in the assessment of the legitimacy of these funds. DD documentation may also provide clear schematics for the DD's approach for each digital asset type to enable the DD's transaction tracing review process to be reconstructed in an auditable manner. Transaction tracing examples include (but are not limited to): (1) assessing whether a digital asset has passed through or interacted with addresses associated with high-risk entities, such as high-risk jurisdictions, mixers or tumblers, privacy wallet(s), unregistered foreign exchanges, darknet marketplaces, ransomware-as-a-service providers; and (2) determining whether on-chain transaction activity appears indicative of certain known high-risk typologies or money laundering techniques (e.g., chain peeling, chain-hopping, etc.).

Customer information collected under the CDD rule may be relevant to other regulatory requirements, including but not limited to, identifying suspicious activity, identifying nominal and beneficial owners of private banking accounts, determining OFAC sanctioned parties, and

[183] Monetary Authority of Singapore, "Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism" (March 2020).

screening unlabeled wallet addresses associated with the customers as appropriate. The DD should define in its policies, procedures and processes how customer information will be used to meet other regulatory requirements. For example, the DD is expected to use the customer information and customer risk profile in its suspicious activity monitoring process to understand the types of transactions a particular customer would normally be expected to engage in as a baseline against which suspicious transactions are identified and to satisfy other regulatory requirements.[184] As discussed above, digital asset analytics should contribute to evaluating the customer's documented intended purposes and expected activity against actual activity through analysis of their source and destination of funds.

The DD may choose to implement CDD policies, procedures, and processes on an enterprise- wide basis. To the extent permitted by law, this implementation may include sharing or obtaining customer information across business lines, separate legal entities within an enterprise, and affiliated support units. To encourage cost effectiveness, enhance efficiency, and increase availability of potentially relevant information, the DD may find it useful to cross-check for customer information in data systems maintained within the financial institution for other purposes, such as credit underwriting, marketing, or frauddetection.

Higher Risk Profile Customers

Customers that pose higher money laundering or terrorist financing risks, (*i.e.,* higher risk profile customers), present increased risk exposure to DDs. As a result, due diligence policies, procedures, and processes should define both when and what additional customer information will be collected based on the customer risk profile and the specific risks posed. Collecting additional information about customers that pose heightened risk, referred to as EDD, for example, in the private and foreign correspondent banking context, is part of an effective due diligence program. DDs should have policies and procedures in place that include the development and maintenance of an accurate and comprehensive list of higher risk profile customers, as well as ensure that such higher risk customers are subject to ongoing and enhanced due diligence. Even within categories of customers with a higher risk profile, there can be a spectrum of risks and the extent to which additional ongoing due diligence measures are necessary may vary on a case-by-case basis. Based on the customer risk profile, the DD may consider obtaining, at account opening (and throughout the relationship), more customer information in order to understand the nature and purpose of the customer relationship, such as:

- Source of wealth.[185]
- Occupation or type of business (of customer or other individuals with ownership or control over the account).

[184] See 31 CFR 1020.210(b)(5)(ii)

[185] Note that the Department includes a risk-focused "source of funds" review, as appropriate, as a requirement of the customer's KYC/onboarding process and ongoing monitoring; accordingly, this reference removes the existing reference within the FFIEC AML Manual to review "source of funds and wealth."

- Financial statements for business customers.
- Common sending/receiving wallet addresses and their exposure to illicit activity.
- Location where the business customer is organized and where they maintain their principal place of business.
- Description of the business customer's primary trade area, whether transactions are expected to be domestic or international, the types of digital asset exchanges the business customer expects to transact with, and the expected volumes of such transactions.
- Description of the business operations, such as total sales, the volume of currency transactions, and information about major customers and suppliers.
- The types of digital asset products and services the customer intends to transact in, as well as the types of digital assets the customer intends to use in such products and services, and the purpose of the selected digital asset mix (e.g., speculative trading, settlement, remittance, etc.).

Source of wealth generally refers to the origin of a customer's entire body of wealth, which is distinct from source of funds. Source of wealth information should provide an informed indication about the size of wealth and how the wealth was acquired. Relevant evidence for source of wealth could include evidence of title, copies of trust deeds, audited accounts, salary details, tax returns and DD statements.[186] In the case of DD customers, source of wealth may also include early holdings in digital assets.

Performing an appropriate level of ongoing due diligence that is commensurate with the customer's risk profile is especially critical in understanding the customer's transactions in order to assist the DD in determining when transactions are potentially suspicious. This determination is necessary for a suspicious activity monitoring system that helps to mitigate the DD's compliance and money laundering risks.

Consistent with the risk-based approach, the DD should do more in circumstances of heightened risk, as well as to mitigate risks generally. Information provided by higher risk profile customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the DD. The DD should establish policies and procedures for determining whether and/or when, on the basis of risk, obtaining and reviewing additional customer information, for example through negative media search programs, would be appropriate.

While not conclusive, certain customer types, such as those found in the "Persons and Entities" section of the FFIEC AML Manual, may pose heightened risk. Besides trusts and other similar corporate/legal structures, art and antiquities market participants (especially those who facilitate transactions), including non-fungible token marketplaces, may pose a higher financial crimes

[186] Monetary Authority of Singapore, "Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism" (March 2020).

risk given the built-in opacity, lack of stable and predictable pricing, and inherent cross-border transportability and/or ease of transfer, thereby making the market vulnerable to illicit value transfer, sanctions evasion, and corruption.[187] In addition, existing laws and regulations may impose, and supervisory guidance may explain expectations for, specific customer due diligence and, in some cases, enhanced due diligence requirements for certain accounts or customers, including foreign correspondent accounts,[188] payable-through accounts,[189] private banking accounts,[190] politically exposed persons,[191] and money services businesses.[192] The DD's risk- based customer due diligence and enhanced due diligence procedures must ensure compliance with these existing requirements and should meet these supervisory expectations.

Ongoing Monitoring of the Customer Relationship

The requirement for ongoing monitoring of the customer relationship reflects existing practices established to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

Therefore, in addition to policies, procedures, and processes for monitoring to identify and report suspicious transactions, the DD's CDD program must include risk-based procedures for performing ongoing monitoring of the customer relationship, on a risk basis, to maintain and update customer information and risk rating (i.e., dynamic risk rating), including beneficial ownership information of legal entity customers.[193] For more information on beneficial ownership of legal entity customers, refer to the "Beneficial Ownership Requirements for Legal Entity Customers" section of the FFIEC AML Manual.

The requirement to update customer information is event-driven and occurs as a result of normal monitoring.[194] Should the DD become aware as a result of its ongoing monitoring that customer information, including beneficial ownership information, has materially changed, it should update the customer information accordingly. Additionally, if this customer information is material and relevant to assessing the risk of a customer relationship, then the DD should reassess the customer

---

[187] White House, "United States Strategy on Countering Corruption" (December 2021); and Treasury, "Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art" (February 2022).

[188] See 31 CFR 1010.610.

[189] See 31 CFR 1010.610(b)(1)(iii).

[190] See 31 CFR 1010.620

[191] Department of State, Department of the Treasury, Federal Reserve, FDIC, OCC, OTS, "Guidance on Enhanced Scrutiny for Transactions that may Involve the Proceeds of Official Corruption" (January 2001).

[192] FinCEN, Federal Reserve, FDIC, NCUA, OCC, OTS, "Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States" (April 2005).

[193] See 31 CFR 1020.210(b)(5)(ii)

[194] Department of the Treasury, FinCEN, "Customer Due Diligence Requirements for Financial Institutions," final rules (RIN 1506-AB25), *Federal Register*, vol. 81, p. 29399 (May 2016).

risk profile/rating and follow established DD policies, procedures, and processes for maintaining or changing the customer risk profile/rating. One common indication of a material change in the customer risk profile is transactions or other activity that are inconsistent with the DD's understanding of the nature and purpose of the customer relationship or with the customer risk profile. Specific to digital assets, ongoing due diligence should include a review of all wallet addresses associated with the customer (including unhosted wallets or hosted wallets from which the customer sends or receives digital assets funds transfers). It should also include the use of digital asset analytics to monitor the activity associated with a customer's wallet(s). Accordingly, Department examiners should assess the DD's policies, processes, and procedures to evaluate whether the DD can demonstrate a consolidated customer view for all inbound and outbound transaction activity for fiat-based transactions as well as each digital asset's activity.

The DD's procedures should establish criteria for when and by whom customer relationships will be reviewed, including updating customer information and reassessing the customer's risk profile. The procedures should indicate who in the organization is authorized to change a customer's risk profile. A number of factors may be relevant in determining when it is appropriate to review a customer relationship including, but not limitedto:

- Significant and unexplained changes in account activity, including deviations in on-chain activity
- Changes in employment or business operation
- Changes in ownership of a business entity
- Red flags identified through suspicious activity monitoring
- Receipt of law enforcement inquiries and requests such as criminal subpoenas, National Security Letters (NSL), and section 314(a) requests
- Receipt of section 314(b) requests or responses, if applicable
- Results of negative media search programs
- Length of time since customer information was gathered and the customer risk profile assessed

The ongoing monitoring element does not impose a categorical requirement that the DD must update customer information on a continuous or periodic basis.[195] However, the DD may establish policies, procedures, and processes for determining whether and when, on the basis of risk, periodic reviews to update customer information should be conducted to ensure that customer information is current and accurate. Given the risks associated with digital assets, DDs should have documented processes highlighting trigger-based events that may warrant customer information review and refresh. DDs should also establish documented processes clarifying the information and analysis required when conducting periodic reviews (e.g., transaction reviews).

[195] Department of the Treasury, FinCEN, "Customer Due Diligence Requirements for Financial Institutions," final rules (RIN 1506-AB25), *Federal Register*, vol. 81, p. 29399 (May 2016).

In addition to the above, DDs should consider the ongoing monitoring of online sources that are known to be used to organize illicit activity, such as the solicitation of money mules, for links to their customers.

3.2.1. Customer Due Diligence – Examination Procedures

Objective. *Assess the DD's compliance with the regulatory requirements for customer due diligence (CDD).*

Procedure	Comments
1. Determine whether the DD has developed and implemented an appropriate written risk-based KYC policy and associated procedures for conducting ongoing CDD (tailored to different customer types) and that they: • Enable the DD to understand the nature and purpose of the customer relationship in order to develop a customer risk profile, including source of funds as appropriate on a risk-focused basis. • Enable the DD to conduct ongoing monitoring for the purpose of identifying and reporting suspicious transactions and, on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers and determination of ownership of wallet address(es) associated with that customer as reasonably possible on a risk-based approach. For example, the Department should generally ensure that DDs should have in place policies, processes, and procedures that demonstrate a consolidated customer view, as reasonably possible, for all inbound and outbound transaction activity for fiat-based transactions as well as each digital asset for which the customer has activity. • Enable the DD to have appropriate triggers in place to determine whether a customer warrants additional due diligence or customer data refresh (e.g.,	

Procedure	Comments
use of a new higher-risk product or service). This includes enabling the DD to follow clear guidelines when conducting periodic reviews (e.g., transaction reviews). • Enable the DD to use customer information and the customer risk profile to understand the types of transactions a particular customer would be expected to engage in and as a baseline against which suspicious transactions are identified.	
2. Determine whether the DD, as part of the overall CDD program, has effective processes to develop customer risk profiles that identify the specific risks of individual customers or categories of customers, including ongoing reviews of customers' wallet address information. Determine whether the process for establishing customer risk profiles includes consideration of high-risk factors, such as geographic risk. Determine whether the DD has policies, processes, and procedures to assess counterparty exposure for virtual currency funds transfers (e.g., beneficiary institutions for outbound transfers). Determine whether the DD has updated its customer risk rating methodology (and model) and incorporated it into the DD's overall risk assessment.	
3. Determine whether the risk-based CDD policies, procedures, and processes are commensurate with the DD's AML/CFT risk profile with increased focus on higher risk customers.	
4. Determine whether the DD has developed and implemented specific processes and procedures for conducting EDD on higher-risk customers.	
5. Determine whether the DD's approach for establishing and applying wallet	

Procedure	Comments
identification criteria and generating related reports are reasonable and clearly identified through policies, processes, and procedures, as well as related reporting.	
6. Determine whether policies, procedures, and processes contain a clear statement of management's and staff's responsibilities, including procedures, authority, and responsibility for reviewing and approving changes to a customer's risk profile, as applicable.	
7. Determine whether the DD has policies, procedures, and processes to identify customers that may pose higher risk for money laundering or terrorist financing that include whether and/or when, on the basis of risk, it is appropriate to obtain and review additional customer information. For example, evaluate whether the DD has developed and maintains a list of higher risk profile customers.	
8. Determine whether the DD provides guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.	
9. Determine whether the DD has a formalized process to conduct quality assurance or quality checks on CDD reviews.	
10. Determine whether the DD has defined in its policies, procedures, and processes how customer information, including beneficial ownership information for legal entity customers (e.g., trusts and other similar arrangements), is used to meet other relevant regulatory requirements, including but not limited to, identifying suspicious activity, identifying nominal and beneficial owners of private banking accounts, and determining OFAC sanctioned parties.	

Procedure	Comments
Transaction Testing	
11. On the basis of a risk assessment, prior examination reports, and a review of the DD's audit findings, select a sample of customer information. Determine whether the DD collects appropriate information sufficient to understand the nature and purpose of the customer relationship and effectively incorporates customer information, including beneficial ownership information for legal entity customers, into the customer risk profile. Transaction testing should include an assessment of the review of source of funds, if appropriate on a risk-focused basis. This sample can be performed when testing the DD's compliance with its policies, procedures, and processes as well as when reviewing transactions or accounts for possible suspicious activity.	
12. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with CDD.	

3.3. Suspicious Activity Reporting – Overview

Objective. *Assess the DD's policies, procedures, and processes, and overall compliance with statutory and regulatory requirements for monitoring, detecting, and reporting suspicious activities. For each digital asset that the DD supports, assess whether the DD's policies, procedures, and processes meet the same standards as for traditional fiat-based activities. Based on overall control processes, provide a consolidated assessment of DD activities for monitoring, detecting, and reporting suspicious activity.*

Suspicious activity reporting forms the cornerstone of the BSA reporting system. It is critical to the United States' ability to utilize financial information to combat terrorism, terrorist financing, money laundering, and other financial crimes. Examiners and DDs should recognize that the quality of SAR content is critical to the adequacy and effectiveness of the suspicious activity reporting system. Therefore, DDs should develop and incorporate processes and procedures for writing high-quality SARs (when appropriate) and should develop processes and procedures for conducing quality control on SAR write-ups before they are filed with FinCEN. These measures are particularly important for DDs due to the global reach and pseudonymous nature of digital assets, both unique inherent features that can be exploited for money laundering and use in illicit activity.

FinCEN and banking regulators recognize that, as a practical matter, it is not possible for a DD to detect and report all potentially illicit transactions that flow through the DD. Accordingly, Department examiners should focus on assessing a DD's policies, procedures, and processes to identify, evaluate, and report suspicious activity. However, as part of the examination process, examiners should review individual SAR filing decisions to determine the effectiveness of the DD's suspicious activity identification, evaluation, and reporting process. Banks, bank holding companies, and their subsidiaries are required by federal regulations[196] to file a SAR with respect to:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating $5,000 (or the equivalent in digital assets)[197] or more when a suspect can be identified.
- Criminal violations aggregating $25,000 (or the equivalent in digital assets) or more regardless of a potential suspect.
- Transactions conducted or attempted by, at, or through the DD (or an affiliate) and

[196] Refer to 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Board of Governors of the Federal Reserve System)(Federal Reserve); 12 CFR 353 (Federal Deposit Insurance Corporation)(FDIC); 12 CFR 748 (National Credit Union Administration)(NCUA); 12 CFR 21.11 and 12 CFR 163.180 (Office of the Comptroller of the Currency)(OCC); and 31 CFR 1020.320 (FinCEN).

[197] Refer to the DD Custody/Fiduciary Manual ("Asset Valuation") for additional background on the Department's approach on valuation techniques for different digital assets. Given the volatility associated with digital assets, DDs may consider these thresholds in the context of each digital asset's historical performance alongside other factors.

aggregating $5,000 (or the equivalent in digital assets) or more, if the DD or affiliate knows, suspects, or has reason to suspect that the transaction:

- May involve potential money laundering or other illegal activity (e.g., terrorism financing).[198]
- Is designed to evade the BSA or its implementing regulations.[199]
- Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the DD knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

A transaction includes a deposit; a withdrawal; a transfer between accounts; an exchange of currency; an extension of credit; a purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security; or any other payment, transfer, or delivery by, through, or to a DD (including virtual currencies).

In the case that the DD is also an MSB, the following SAR-filing thresholds and requirements apply per FinCEN:[200]

- For transactions conducted or attempted by, at or through a money services business or its agent, the threshold of $2,000 applies;
- For transactions identified by issuers of money orders or traveler's checks from a review of clearance records or other similar records of instruments that have been sold or processed, the threshold of $5,000 applies; and
- MSBs have 30 days after becoming aware of a suspicious transaction to complete and file the SAR MSB form.

Safe Harbor for Banks From Civil Liability for Suspicious Activity Reporting

Federal law (31 USC 5318(g)(3)) provides protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to the SAR instructions. Specifically, the law provides that a DD and its directors, officers, employees, and agents that make a disclosure to the appropriate authorities of any possible violation of law or regulation, including a disclosure in connection with the preparation of SARs, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the

[198] FinCEN issued guidance identifying certain BSA expectations for DDs offering services to marijuana- related businesses, including expectations for filing SARs, FIN-2014-G001, February 14, 2014.

[199] Refer to the FFIEC AML Manual's Appendix G ("Structuring") for additional guidance.

[200] FinCEN, "Money Services Business (MSB) Suspicious Activity Reporting."

disclosure." The safe harbor applies to SARs filed within the required reporting thresholds as well as to SARs filed voluntarily on any activity below the threshold.[201]

Systems to Identify, Research, and Report Suspicious Activity

Suspicious activity monitoring and reporting are critical internal controls. Proper monitoring and reporting processes are essential to ensuring that the DD has an adequate and effective BSA compliance program. Appropriate policies, procedures, and processes should be in place to monitor and identify unusual activity. The sophistication of monitoring systems should be dictated by the DD's risk profile, with particular emphasis on the composition of higher-risk products, services, customers, entities, and geographies. The DD should ensure adequate staff is assigned to the identification, research, and reporting of suspicious activities, taking into account the DD's overall risk profile and the volume of transactions. Monitoring systems typically include employee identification or referrals, transaction-based (manual) systems, surveillance (automated) systems, or any combination of these.

The U.S. Treasury's 2022 National Risk Assessments noted that "AML/CFT-related deficiencies identified by the OCC [partly] stem from… ineffective processes related to suspicious activity monitoring and reporting, including the timeliness and accuracy of SAR filings."[202] Therefore, it is critical for DDs to have processes and controls in place for effective suspicious activity monitoring and reporting systems, which generally include five key components. The components, listed below are interdependent, and an effective suspicious activity monitoring and reporting process should include successful implementation of each component.

[201] The agencies incorporated the statutory expansion of the safe harbor by cross-referencing section 5318(g) in their SAR regulations. The OCC and FinCEN amended their SAR regulations to make clear that the safe harbor also applies to a disclosure by a DD made jointly with another financial institution for purposes of filing a joint SAR (see 12 CFR 21.11(l) and 31 CFR 1020.320(e)), respectively.

[202] U.S. Treasury, "National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing" (March 2022).

Illustrative Example: Key Suspicious Activity Monitoring Components

Identification of Unusual Activity	Alert Management	SAR Decision Making	SAR Completion & Filing	Monitoring & SAR Filing on Continuing Activity
May include employee identification, law enforcement inquiries, other referrals, transaction and surveillance monitoring, and **digital asset analytics system output**. Digital asset analytics tools are especially helpful in identifying the owner(s) of digital asset wallets, determining the risk profile of digital asset wallets, and ingesting transaction data from the underlying blockchain to facilitate transaction monitoring. DDIs should also use digital asset analytics to trace incoming and outgoing transactions to wallet addresses. Potential unusual activity should be **escalated and/or reported immediately, in accordance with the DDI's processes**.	Focuses on processes used to investigate and evaluate identified unusual activity. DDIs should have policies, procedures, and processes in place—with clear timelines—for referring unusual activity from all areas of the DDI or business lines to the personnel or department responsible for evaluating unusual activity. Processes and documentation should include the use of **alert and case investigations, case management tools, CDD and EDD information, external research tools (e.g., open-source intelligence reviews, negative news screening, etc.), as well as red flag indicators particularly relevant for illicit activity involving the use of digital assets**.	The decision maker, whether an individual or committee, should have the authority to make the final SAR filing decision. The DDI should have clearly defined processes and procedures for SAR filing decisions, whether they are made by an individual or a committee. DDIs should document SAR decisions, including the specific reason for filing or not filing a SAR. Thorough documentation provides a record of the SAR decision-making process, including final decisions not to file a SAR. **DDIs should remember that, like traditional banks, they are obligated to comply with SAR reporting requirements under the BSA.**	Appropriate policies, procedures, and processes should be in place to ensure SARs are filed in a complete, accurate, and timely manner, and that the narrative provides a sufficient description of the activity reported as well as the basis for filing. Information especially useful for **SARs involving digital asset transactions includes virtual currency wallet addresses, transaction details and relevant transaction history, available login information (e.g., IP address), and mobile device information**. DDIs should file SARs no later than **30 calendar days** from the date of the initial detection; if no suspect can be identified, the time period for filing is extended to **60 days**.	The DDI should develop policies, procedures, and processes indicating when to escalate issues or problems identified as the result of repeat SAR filings on accounts. For continuing suspicious activity, DDIs should file a report **at least every 90 calendar days**. DDIs with SAR requirements are also permitted to file SARs for continuing activity after a **90-day review with the filing deadline being 120 calendar days after** the date of the previously related SAR filing; they **may also file SARs on continuing activity earlier than the 120-day deadline** if the they believe the activity warrants earlier review by law enforcement.

Breakdowns in any one or more of these components may adversely affect SAR reporting and BSA compliance. The five key components to an effective monitoring and reporting system are:

- Identification or alert of unusual activity (which may include employee identification, law enforcement inquiries, other referrals, transaction and surveillance monitoring, and digital asset analytics[203] system output).
- Managing alerts.
- SAR decision making.
- SAR completion and filing.[204]
- Monitoring and SAR filing on continuing activity.

These components are present in DDs of all sizes. However, the structure and formality of the components may vary. Larger DDs typically have greater differentiation and distinction between functions and may devote entire departments to the completion of each component. Smaller DDs may use one or more employees to complete several tasks (e.g., review of monitoring reports, research activity, and completion of the actual SAR). Policies, procedures, and processes should

[203] See section *3.4. Digital Asset Analytics* for additional information on the use of analytics providers to conduct identification or alerts of unusual activity.

[204] The U.S. Treasury 2022 National Risk Assessment highlighted the importance of an effective process related to suspicious activity monitoring and the timeliness and accuracy of SAR filings.

describe the steps the DD takes to address each component and indicate the person(s) or departments responsible for identifying or producing an alert of unusual activity, managing the alert, deciding whether to file, SAR completion and filing, and monitoring and SAR filing on continuing activity.

Identification of Unusual Activity

DDs use a number of methods to identify potentially suspicious activity, including but not limited to activity identified by employees during day-to-day operations, law enforcement inquiries, or requests, such as those typically seen in section 314(a) and section 314(b) requests, advisories issued by regulatory or law enforcement agencies, transaction and surveillance monitoring (including digital asset analytics) system outputs, or any combination of these.

Digital assets present unique challenges for the identification of unusual activity. Transaction data stored on the blockchain ledger (or "on-chain") typically includes identifying information such as sender/receiver wallet addresses, time and date, and value of the transaction; however, this information is generally pseudonymous, meaning the transaction details do not indicate the identities of the originator, beneficiary, or underlying beneficial owners.

Due to these unique characteristics, DDs require digital asset analytics tools to: 1) identify the owner(s) of digital asset wallets as reasonably possible, 2) determine the risk profile of digital asset wallets, and 3) ingest transaction data from the underlying blockchain to facilitate manual or automated transaction monitoring. Additionally, as it can be difficult to identify underlying ownership of a digital asset wallet, it is critical for DDs to trace incoming and outgoing transactions (through blockchain analytics or additional means) to wallet addresses whose owner(s) can be identified with reasonable certainty on a risk-focused basis. FinCEN has encouraged financial institutions to share information with one another in order to better identify and report potential money laundering and other illicit activities. DDs that participate in section 314(b) shall notify FinCEN and establish policies, procedures, and processes for sharing and receiving information.

Given the ability of criminal actors to "misuse virtual assets, [which] exploits and undermines their innovative potential, including through laundering of illicit proceeds," FinCEN is in particular encouraging "covered institutions to share [potential suspicious activity information] with one another... in order to better identify and report potential money laundering or terrorist financing."[205] Therefore, if a DD decides to voluntarily participate in section 314(b), it is critical that it notifies FinCEN of its participation and also develops policies, procedures, and processes for sharing and receiving information that takes into account digital asset-specific nuances.

[205] FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities" (June 2021).

Employee Identification

During the course of day-to-day operations, employees may observe unusual or potentially suspicious transaction activity. DDs should implement appropriate training, policies, and procedures to ensure that personnel adhere to the internal processes for identification and referral of potentially suspicious activity. DDs should be aware of all methods of identification and should ensure that their suspicious activity monitoring system includes processes to facilitate the transfer of internal referrals to appropriate personnel for further research for both traditional fiat-based activity and digital assets.

Law Enforcement Inquiries and Requests

DDs should establish policies, procedures, and processes for identifying subjects of law enforcement requests, monitoring the transaction activity of those subjects when appropriate, identifying unusual or potentially suspicious activity related to those subjects, and filing, as appropriate, SARs related to those subjects. Law enforcement inquiries and requests can include grand jury subpoenas, National Security Letters (NSL), and section 314(a) requests.[206] Such policies, procedures, and processes should be distinct from traditional DD law enforcement inquiries and requests policies, procedures, and processes, in that they consider and include digital asset-specific nuances, risks, and information.

Mere receipt of any law enforcement inquiry does not, by itself, require the filing of a SAR by the DD. Nonetheless, a law enforcement inquiry may be relevant to a DD's overall risk assessment of its customers and accounts. For example, the receipt of a grand jury subpoena should cause a DD to review account activity for the relevant customer.[207] A DD should assess all of the information it knows about its customer, including the receipt of a law enforcement inquiry, in accordance with its risk-based AML/CFT compliance program.

The DD should determine whether a SAR should be filed based on all customer information available. Due to the confidentiality of grand jury proceedings, if a DD files a SAR after receiving a grand jury subpoena, law enforcement discourages DDs from including any reference to the receipt or existence of the grand jury subpoena in the SAR. Rather, the SAR should reference only those facts and activities that support a finding of suspicious transactions identified by the DD.

---

[206] Refer to core overview section, "Information Sharing," of the FFIEC AML Manual, for a discussion on section 314(a) requests.

[207] Bank Secrecy Act Advisory Group, "Section 5 – Issues and Guidance" *The SAR Activity Review – Trends, Tips & Issues*, Issue 10, on the FinCEN Web site (May 2006).

National Security Letters

NSLs are written investigative demands that may be issued by the local Federal Bureau of Investigation (FBI) and other federal governmental authorities in counterintelligence and counterterrorism investigations to obtain the following:

- Telephone and electronic communications records from telephone companies and Internet service providers.[208]
- Information from credit bureaus.[209]
- Financial records from financial institutions.[210]

NSLs are highly confidential documents; for that reason, examiners do not review or sample specific NSLs.[211] Pursuant to 12 USC 3414(a)(3) and (5)(D), no DD, or officer, employee or agent of the institution, can disclose to any person that a government authority or the FBI has sought or obtained access to records through a Right to Financial Privacy Act NSL. DDs that receive NSLs must take appropriate measures to ensure the confidentiality of the letters and should have procedures in place for processing and maintaining the confidentiality of NSLs.

If a DD files a SAR after receiving a NSL, the SAR should not contain any reference to the receipt or existence of the NSL. The SAR should reference only those facts and activities that support a finding of unusual or suspicious transactions identified by the DD.

Questions regarding NSLs should be directed to the DD's local FBI field office. Contact information for the field offices can be found at www.fbi.gov.

Transaction Monitoring (Manual Transaction Monitoring)

A transaction monitoring system, sometimes referred to as a manual transaction monitoring system, typically targets specific types of transactions (e.g., those involving large amounts of cash, those to or from foreign geographies) and includes a manual review of various reports generated by the DD's MIS or vendor systems in order to identify unusual activity. DDs should have policies, processes, and procedures in place to generate reports for each type of activity (including for each digital asset) the DD supports to detect unusual activity.

Examples of MIS reports include currency activity reports, funds transfer reports (including virtual currency funds transfer reports or exception reports), monetary instrument sales reports, large item reports, significant balance change reports, ATM transaction reports, and nonsufficient funds

---

[208] Electronic Communications Privacy Act, 18 USC 2709.

[209] Fair Credit Reporting Act, 15 USC 1681.

[210] Right to Financial Privacy Act of 1978, 12 USC 3401 *et seq.*

[211] Refer to the Bank Secrecy Act Advisory Group, *The SAR Activity Review – Trends, Tips & Issues*, Issue 8, April 2005 for further information on NSLs which is available on the FinCEN Web site.

(NSF) reports. Many MIS or vendor systems include filtering models for identification of potentially unusual activity. The process may involve review of daily reports, reports that cover a period of time (e.g., rolling 30-day reports, monthly reports), or a combination of both types of reports. The type and frequency of reviews and resulting reports used should be commensurate with the DD's AML/CFT risk profile and appropriately cover its higher-risk products, services, customers, entities, and geographic locations.

MIS or vendor system-generated reports typically use a discretionary dollar threshold. Thresholds selected by management for the production of transaction reports should enable management to detect unusual activity. Upon identification of unusual activity, assigned personnel should review CDD and other pertinent information to determine whether the activity is suspicious. Management should periodically evaluate the appropriateness of filtering criteria and thresholds used in the monitoring process. Each DD should evaluate and identify filtering criteria most appropriate for their DD. In the context of digital assets, DDs should have clearly documented processes through which they verify that filtering criteria and associated thresholds for traditional ML/TF and OFAC typologies are in place. DDs should similarly demonstrate that manual or automated controls are in place for typologies specific to the DD's risk profile and the digital assets the DD supports. Additionally, it is critical that DDs evidence appropriately tailored transaction monitoring coverage against applicable typologies and red flags (e.g., through conducting a coverage assessment), such as the identification of deviations from the profile of a customer's intended purposes.[212] The programming of the DD's monitoring systems should be independently reviewed for reasonable filtering criteria. Typical transaction monitoring reports are as follows.

Currency activity reports. Most vendors offer reports that identify all currency activity or currency activity greater than $10,000 (or the equivalent in digital assets). These reports assist bankers with filing CTRs and identifying suspicious currency activity. DDs may also be subject to Virtual Currency Transaction Report ("VCTR") filing requirements under federal regulation.[213] Most DD information service providers offer currency activity reports that can filter transactions using various parameters, for example:

- Currency activity including multiple transactions greater than $10,000 (or the equivalent in digital assets and involving unhosted wallets, where applicable and required under federal regulation, or wallets hosted in a FinCEN-identified jurisdiction).
- Currency activity (single and multiple transactions) below the $10,000 reporting requirement (e.g., between $7,000 and $10,000) (or the equivalent in digital assets and involving unhosted wallets, where applicable and required under federal regulation, or wallets hosted in a FinCEN-identified jurisdiction).

[212] New York Department of Financial Services, "Guidance on Use of Blockchain Analytics" (April 2022).

[213] FinCEN Proposed Rule, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" (January 2021). In a proposed rule published in January 2021, FinCEN recommended extending transaction reporting requirements to "certain transactions involving convertible virtual currency ("CVC") or digital assets with legal tender status ("legal tender digital assets" or "LTDA")." Such VCTRs would be submitted on a Value Transaction Report form similar to the existing FinCEN CTR form.

- Currency transactions involving multiple lower dollar (or lower digital assets) transactions (e.g., $3,000) that over a period of time (e.g., 15 days) aggregate to a substantial sum of money (e.g., $30,000 or the equivalent in digital assets and involving unhosted wallets, where applicable and required under federal regulation, or wallets hosted in a FinCEN-identified jurisdiction).
- Currency transactions aggregated by customer name, taxpayer identification number, or customer information file number.

Such filtering reports, whether implemented through a purchased vendor software system or through requests from information service providers, significantly enhance a DD's ability to identify and evaluate unusual currency transactions.

Funds transfer records. The BSA requires DDs to maintain records of funds transfers in amounts of $3,000 and above. FinCEN published a proposed rule in January 2021 that, if enacted, would establish "new recordkeeping requirements for certain CVC or LTDA (i.e., legal tender digital assets) transactions that is similar to the recordkeeping and travel rule regulations pertaining to funds transfers and transmittals of funds."[214] Periodic review of this information can assist DDs in identifying patterns of unusual activity. A periodic review of the funds transfer records in DDs with low funds transfer activity is usually sufficient to identify unusual activity. For DDs with more significant funds transfer activity, use of spreadsheet or vendor software is an efficient way to review funds transfer activity for unusual patterns. Most vendor software systems include standard suspicious activity filter reports. These reports typically focus on identifying certain higher-risk geographic locations and larger dollar funds transfer transactions for individuals and businesses. Each DD should establish its own filtering criteria. Noncustomer funds transfer transactions and payable upon proper identification (PUPID) transactions should be reviewed for unusual activity. Activities identified during these reviews should be subjected to additional research to ensure that identified activity is consistent with the stated account purpose and expected activity. When inconsistencies are identified, DDs may need to conduct a global relationship review to determine if a SAR is warranted.

Refer to the *3.7. Virtual Currency Funds Transfers Recordkeeping* for more information on digital asset-specific considerations for funds transfers compliance and *3.2. Customer Due Diligence* for ongoing monitoring of the customer relationship.

Surveillance Monitoring (Automated Account Monitoring)

A surveillance monitoring system, sometimes referred to as an automated account monitoring system, can cover multiple types of transactions and use various rules to identify potentially suspicious activity. In addition, many can adapt over time based on historical activity, trends, or internal peer comparison. These systems typically use computer programs, developed in-house or

[214] FinCEN Proposed Rule, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" (January 2021).

purchased from vendors, to identify individual transactions, patterns of unusual activity, or deviations from expected activity. These systems can capture a wide range of account activity, such as deposits, withdrawals, funds transfers, automated clearing house (ACH) transactions, and automated teller machine (ATM) transactions, directly from the DD's core data processing system. DDs that are large, operate in many locations, or have a large volume of higher-risk customers typically use surveillance monitoring systems. For fiat-based products and services, surveillance monitoring systems typically ingest data from the DD's core banking system(s); however, in the context of digital assets DDs may leverage advancements in distributed ledger technology for transparency and traceability,[215] such as blockchain analytics capabilities to obtain and enhance transaction data that may exist on the blockchain in order to perform surveillance monitoring. Department examiners should assess the DD's overall typologies taking these features into account to determine whether the DD has sufficient coverage for both traditional money laundering typologies as well as typologies specific to digital assets. To the degree that DDs outsource transaction monitoring of on-chain activity, they should have clearly documented policies, processes, and procedures clarifying how the blockchain analytics activity integrates into the DD's overall control framework.[216]

Surveillance monitoring systems include rule-based and intelligent systems. Rule-based systems detect unusual transactions that are outside of system-developed or management- established "rules." Such systems can consist of few or many rules, depending on the complexity of the in-house or vendor product. These rules are applied using a series of transaction filters or a rules engine. Rule-based systems are more sophisticated than the basic manual system, which only filters on one rule (e.g., transaction greater than $10,000). Rule-based systems can apply multiple rules, overlapping rules, and filters that are more complex. For example, rule-based systems can initially apply a rule, or set of criteria to all accounts within a DD (e.g., all retail customers), and then apply a more refined set of criteria to a subset of accounts or risk category of accounts (e.g., all retail customers with direct deposits). Rule-based systems can also filter against individual customer-account profiles.

Intelligent systems are adaptive and can filter transactions, based on historical account activity or compare customer activity against a pre-established peer group or other relevant data. Intelligent systems review transactions in context with other transactions and the customer profile. In doing so, these systems increase their information database on the customer, account type, category, or business, as more transactions and data are stored in the system.

Relative to surveillance monitoring, system capabilities and thresholds refer to the parameters or filters used by DDs in their monitoring processes. Parameters and filters should be reasonable and tailored to the activity that the DD is trying to identify or control. After parameters and filters have been developed, they should be reviewed before implementation to identify any gaps (common money laundering techniques or frauds) that may not have been addressed. For example,

---

[215] White House, "United States Strategy on Countering Corruption" (December 2021).

[216] New York Department of Financial Services, "Guidance on Use of Blockchain Analytics" (April 2022).

a DD may discover that its filter for cash structuring is triggered only by a daily cash transaction in excess of $10,000 (or the equivalent in digital assets). The DD may need to refine this filter in order to avoid missing potentially suspicious activity because common cash structuring techniques often involve transactions that are slightly under the CTR threshold. DDs should also conduct periodic reviews of parameters and filters to any digital asset analytics or surveillance monitoring solutions consistent with the DD's risk profile. If the DD uses digital asset analytics providers to detect suspicious digital asset transaction activity, the DD may need to refine their filters and parameters depending on the risks associated with the specific digital assets being monitored against the DD's stated risk appetite. Refer to *3.8. Model Risk Management for DDs — Overview* for more a detailed discussion around model risk management for surveillance monitoring.

Once established, the DD should review and test system capabilities and thresholds on a periodic basis. This review should focus on specific parameters or filters in order to ensure that intended information is accurately captured and that the parameter or filter is appropriate for the DD particular risk profile.

Understanding the filtering criteria of a surveillance monitoring system is critical to assessing the effectiveness of the system. System filtering criteria should be developed through a review of specific higher-risk products and services, customers and entities, and geographies. System filtering criteria, including specific profiles and rules, should be based on what is reasonable and expected for each type of account. Monitoring accounts purely based on historical activity can be misleading if the activity is not actually consistent with similar types of accounts. For example, an account may have a historical transaction activity that is substantially different from what would normally be expected from that type of account (e.g., an individual customer depositing large sums of digital assets from multiple wallet addresses, indicative of performing unregistered money transmission or facilitating money laundering).

The authority to establish or change expected activity profiles should be clearly defined through policies and procedures. Controls should ensure limited access to the monitoring systems, and changes should generally require the approval of the BSA compliance officer or senior management. Management should document and be able to explain filtering criteria, thresholds used, and how both are appropriate for the DD's risks. Management should also periodically review and test the filtering criteria and thresholds established to ensure that they are still effective. In addition, the monitoring system's programming methodology and effectiveness should be independently validated to ensure that the models are detecting potentially suspicious activity. The independent validation should also verify the policies in place and that management is complying with those policies. Where a DD relies on third-party model(s), it is ultimately responsible for complying with AML/CFT requirements. While the proprietary nature of third-party models is a consideration, sound risk management practices include obtaining sufficient information from the third party to understand how the model operates and performs, ensuring that it is working as expected, and tailoring its use to the unique risk profile of the DD. In addition, it is important that DDs using third-party models have contingency plans if the third-party model is no longer

available or serviced or may no longer be reliable.[217] Refer to *Section 3.8* on Model Risk Management for more details.

Digital Asset Analytics Applications for Identifying Suspicious Activity

DDs must ensure that all products and services (including digital assets) are subject to transaction and surveillance monitoring. Digital assets, and their supporting infrastructure, create challenges to traditional approaches to compliance with and enforcement of AML/CFT and OFAC requirements. The transaction data for digital assets is often publicly available on the underlying blockchain; however, this data must be ingested and enhanced in order to conduct surveillance monitoring. Digital asset analytics tools have emerged to support transaction monitoring and surveillance of digital asset transactions through a number of distinct features.

However, these capabilities alone may not always be sufficient for monitoring against all applicable AML/CFT and OFAC-related transaction and surveillance monitoring typologies. Further risk-based controls may be necessary depending on the circumstances of a particular institution (including pairing blockchain analytics with behavioral analytics for traditional typologies coverage).

Refer to *3.6. Digital Asset Analytics — Overview* for more information about digital asset-specific considerations for digital asset analytics and surveillance solutions.

Managing Alerts

Alert management focuses on processes used to investigate and evaluate identified unusual activity. DDs should be aware of all methods of identification and should ensure that their suspicious activity monitoring program includes processes to evaluate any unusual activity identified, regardless of the method of identification. DDs should have policies, procedures, and processes in place for referring unusual activity from all areas of the DD or business lines to the personnel or department responsible for evaluating unusual activity.

Within those procedures, management should establish a clear and defined escalation process from the point of initial detection to disposition of the investigation.

The DD should assign adequate staff to the identification, evaluation, and reporting of potentially suspicious activities, taking into account the DD's overall risk profile and the volume of transactions. Additionally, a DD should ensure that the assigned staff possess the requisite experience levels and are provided with comprehensive and ongoing training to maintain their

[217] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, "Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance" (April 2021).

expertise. Staff should also be provided with sufficient internal and external tools to allow them to properly research activities and formulate conclusions.

Internal research tools include, but are not limited to, access to account systems and account information, including CDD and EDD information. CDD and EDD information assist DDs in evaluating if the unusual activity is considered suspicious. For additional information, refer to the core overview section, *3.2. Customer Due Diligence*. External research tools may include widely available Internet media search tools, as well those accessible by subscription. For example, DDs may use open-source intelligence ("OSINT") data as part of the investigations process.[218] After thorough research and analysis, investigators should document conclusions including any recommendation regarding whether or not to file a SAR.

When multiple departments are responsible for researching unusual activities (i.e., the BSA department researches BSA-related activity and the Fraud department researches fraud- related activity), the lines of communication between the departments must remain open.

This allows DDs with bifurcated processes to gain efficiencies by sharing information, reducing redundancies, and ensuring all suspicious activity is identified, evaluated, and reported.

If applicable, reviewing and understanding suspicious activity monitoring across the organizations' affiliates, subsidiaries, and business lines may enhance a banking organization's ability to detect suspicious activity, and thus minimize the potential for financial losses, increased legal or compliance expenses, and reputational risk to the organization. Refer to the expanded overview section, FFIEC AML Manual's "AML/CFT Compliance Program Structures," for further guidance.

Identifying Underlying Crime

DDs are required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing,[219] and certain other crimes above prescribed dollar thresholds.

However, DDs are not obligated to investigate or confirm the underlying crime (e.g., terrorist financing, money laundering, tax evasion, identity theft, and various types of fraud). Investigation is the responsibility of law enforcement. When evaluating suspicious activity and completing the SAR, DDs should, to the best of their ability, identify the characteristics of the suspicious activity. Suspicious Activity Information, Part II of the SAR provides a number of categories with different types of suspicious activity. Within each category, there is the option of selecting "Other" if none

[218] White House, "United States Strategy on Countering Corruption" (December 2021).

[219] If a DD knows, suspects, or has reason to suspect that a customer may be linked to terrorist activity against the United States, the DD should immediately call FinCEN's Financial Institutions terrorist hot line toll-free number (866) 556-3974. Similarly, if any other suspected violation — such as an ongoing money laundering scheme — requires immediate attention, the DD should notify the appropriate federal banking and law enforcement agencies. In either case, the DD must also file a SAR.

of the suspicious activities apply. However, the use of "Other" should be limited to situations that cannot be broadly identified within the categories provided.

SAR Decision Making

After thorough research and analysis has been completed, findings are typically forwarded to a final decision maker (individual or committee) in a timely manner. The DD should have policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity. Within those procedures, management should establish a clear and defined escalation process from the point of initial detection to disposition of the investigation.

The decision maker, whether an individual or committee, should have the authority to make the final SAR filing decision. When the DD uses a committee, there should be a clearly defined process to resolve differences of opinion on filing decisions and completed in a timely manner. DDs should document SAR decisions, including the specific reason for filing or not filing a SAR. Thorough documentation provides a record of the SAR decision-making process, including final decisions not to file a SAR. However, due to the variety of systems used to identify, track, and report suspicious activity, as well as the fact that each suspicious activity reporting decision is based on unique facts and circumstances, no single form of documentation is required when a DD decides not to file.[220]

The decision to file a SAR is an inherently subjective judgment. Examiners should focus on whether the DD has an effective SAR decision-making process, not individual SAR decisions. Examiners may review individual SAR decisions as a means to test the effectiveness of the SAR monitoring, reporting, and decision-making process. In those instances where the DD has an established SAR decision-making process, has followed existing policies, procedures, and processes, and has determined not to file a SAR, the DD should not be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.[221]

SAR Filing on Continuing Activity

One purpose of filing SARs is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. This objective is accomplished by the filing of a SAR that identifies the activity of concern. If this activity continues over a period of time, such information should be made known to law enforcement and Department/federal banking agencies. FinCEN's guidelines have suggested that DDs should report continuing suspicious activity by filing a report at least every 90 calendar days.

---

[220] Bank Secrecy Act Advisory Group, "Section 4 – Tips on SAR Form Preparation & Filing," *The SAR Activity Review – Trends, Tips & Issues*, Issue 10, May 2006, page 38, on the FinCEN Web site.

[221] Refer to the FFIEC AML Manual's Appendix R ("Interagency Enforcement Statement") for additional information.

Subsequent guidance permits DDs with SAR requirements to file SARs for continuing activity after a 90-day review with the filing deadline being 120 calendar days after the date of the previously related SAR filing. DDs may also file SARs on continuing activity earlier than the 120-day deadline if the DD believes the activity warrants earlier review by law enforcement.[222] This practice notifies law enforcement of the continuing nature of the activity in aggregate. In addition, this practice reminds the DD that it should continue to review the suspicious activity to determine whether other actions may be appropriate, such as DD management determining that it is necessary to terminate a relationship with the customer or employee that is the subject of the filing.

DDs should be aware that law enforcement may have an interest in ensuring that certain accounts remain open notwithstanding suspicious or potential criminal activity in connection with those accounts. If a law enforcement agency requests that a DD maintain a particular account, the DD should ask for a written request. The written request should indicate that the agency has requested that the DD maintain the account and the purpose and duration of the request. Ultimately, the decision to maintain or close an account should be made by a DD in accordance with its own standards and guidelines.[223]

The DD should develop policies, procedures, and processes indicating when to escalate issues or problems identified as the result of repeat SAR filings on accounts. The procedures should include:

- Review by senior management and legal staff (e.g., BSA compliance officer or SAR committee).
- Criteria for when analysis of the overall customer relationship is necessary.
- Criteria for whether and, if so, when to close the account.
- Criteria for when to notify law enforcement, if appropriate.

SAR Completion and Filing

SAR completion and filing are a critical part of the SAR monitoring and reporting process. Appropriate policies, procedures, and processes should be in place to ensure SARs are filed in a timely manner, are complete and accurate, and that the narrative provides a sufficient description of the activity reported as well as the basis for filing. FinCEN developed a new electronic BSA Suspicious Activity Report (BSAR) that replaced FinCEN SAR-DI form TD F 90-22.47. The BSAR provides a uniform data collection format that can be used across multiple industries. As of April 1, 2013, the BSAR is mandatory and must be filed through FinCEN's BSA E-Filing System. The BSAR does not create or otherwise change existing statutory and regulatory expectations for DDs.

---

[222] Refer to Frequently Asked Questions Regarding the FinCEN Suspicious Activity Report, Question #16.

[223] Refer to "Requests by Law Enforcement for Financial Institutions to Maintain Accounts" (June 2007).

The BSAR includes a number of additional data elements pertaining to the type of suspicious activity and the financial services involved. Certain fields in the BSAR are marked as "critical" for technical filing purposes. This means the BSA E-Filing System does not accept filings in which these fields are left blank. For these items, the DD must either provide the requested information or check the "unknown" box that is provided with each critical field.

DDs should provide the most complete filing information available consistent with existing regulatory expectations, regardless of whether or not the individual fields are deemed critical for technical filing purposes.[224]

DDs should report the information that they know, or that otherwise arises, as part of their case reviews. Other than the critical fields, the addition of the new and expanded data elements does not create an expectation that DDs will revise internal programs, or develop new programs, to capture information that reflects the expanded lists.[225] Refer to Appendix T of the FFIEC AML Manual for additional information on filing through the BSA E-Filing System.

In its 2019 *Advisory on Illicit Activity Involving Convertible Virtual Currency* guidance, FinCEN clarified that virtual currency transactions "generate a significant variety of information elements that may be extremely useful to law enforcement and other national security agencies in investigating potential illicit conduct involving CVC transactions." [226] Specifically, the information includes the customer's:

- virtual currency wallet addresses;
- whether the transaction involved an unhosted wallet;
- account information;
- transaction details (including virtual currency transaction hash and information on the originator and the recipient);
- relevant transaction history;
- available login information (including IP addresses, geolocation, use of VPN);
- mobile device information (such as device IMEI);
- information obtained from analysis of the customer's public online profile and communications.

In this guidance, FinCEN also clarified that a DD's SAR-filing guidance should include the need to reference the "CVC FIN-2019-A003" advisory in SARs related to possible illicit activity involving CVC (or digital assets). Additionally, where activity heavily implicates digital assets,

---

[224] FinCEN, "Filing FinCEN's new Currency Transaction Report and Suspicious Activity Report," FIN-2012-G002 (March 2012).

[225] *Id*.

[226] FinCEN, "Advisory on Illicit Activity Involving Convertible Virtual Convertible Virtual Currency" (May 2019). Note that FinCEN has also provided additional cyber-related guidance for consideration, including "FIN-2016-A005: Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime" (October 2016) and "FinCEN Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the COVID-19 Pandemic" (July 2020).

such as in the case of ransomware, specific FinCEN filing requirements also apply.[227] Accordingly, DDs should assess existing guidance on SARs specific to virtual currencies and digital assets as part of their policies, processes, and procedures for law enforcement inquiries and requests. As part of this review, Department examiners should confirm the DD's approach to SAR filings related to non-AML activity, for example fraud or market manipulation. Examiners should also evaluate whether a DD has developed processes and procedures for conducting quality control and/or quality assurance on SAR narratives before they are filed.

Note: DDs should also be aware of the OFAC reporting requirements that exist (i.e., in certain cases, blocked reports are required in addition to filing SARs with FinCEN).

Timing of a SAR Filing

The SAR rules require that a SAR be electronically filed through the BSA E-Filing System no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect can be identified, the time period for filing a SAR is extended to 60 days. Organizations may need to review transaction or account activity for a customer to determine whether to file a SAR. The need for a review of customer activity or transactions does not necessarily indicate a need to file a SAR. The time period for filing a SAR starts when the organization, during its review or because of other factors, knows or has reason to suspect that the activity or transactions under review meet one or more of the definitions of suspicious activity.[228]

The phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review. There are a variety of legitimate transactions that could raise a red flag simply because they are inconsistent with an accountholder's normal account activity.

For example, a real estate investment (purchase or sale), the receipt of an inheritance, or a gift, may cause an account to have a significant credit or debit that would be inconsistent with typical account activity. The DD's automated account monitoring system or initial discovery of information, such as system-generated reports, may flag the transaction; however, this should not be considered initial detection of potential suspicious activity. The 30-day (or 60-day) period does not begin until an appropriate review is conducted, and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR regulation.[229]

Whenever possible, an expeditious review of the transaction or the account is recommended and can be of significant assistance to law enforcement. In any event, the review should be completed

---

[227] FinCEN, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," (November 2021).

[228] Bank Secrecy Act Advisory Group, "Section 5 – Issues and Guidance," *The SAR Activity Review – Trends, Tips & Issues*, Issue 1 (October 2000).

[229] Bank Secrecy Act Advisory Group, "Section 5 – Issues and Guidance," *The SAR Activity Review – Trends, Tips & Issues*, Issue 10, page 44 (May 2006). For examples of when the date of initial detection occurs, refer to *SAR Activity Review – Trends, Tips, and Issues,* Issue 14 (October 2008).

in a reasonable period of time. What constitutes a "reasonable period of time" varies according to the facts and circumstances of the particular matter being reviewed and the effectiveness of the SAR monitoring, reporting, and decision-making process of each DD. The key factor is that a DD has established adequate procedures for reviewing and assessing facts and circumstances identified as potentially suspicious, and that those procedures are documented and followed.[230]

For situations requiring immediate attention, in addition to filing a timely SAR, a DD must immediately notify, by telephone, an "appropriate law enforcement authority" and, as necessary, the Department. For this initial notification, an "appropriate law enforcement authority" would generally be the local office of the IRS Criminal Investigation Department or the FBI. For any OFAC filings, the Department also requires that the DD also provide prompt notice to the Department. Notifying law enforcement of a suspicious activity does not relieve a DD of its obligation to file a SAR.[231]

SAR Quality

DDs are required to file SARs that are complete, thorough, and timely. DDs should include all known subject information on the SAR. The importance of the accuracy of this information cannot be overstated. Inaccurate information on the SAR, or an incomplete or disorganized narrative, may make further analysis difficult, if not impossible. However, there may be legitimate reasons why certain information may not be provided in a SAR, such as when the filer does not have the information. A thorough and complete narrative may make the difference in determining whether the described conduct and its possible criminal nature are clearly understood by law enforcement. Because the SAR narrative section is the only area summarizing suspicious activity, the section, as stated on the SAR, is "critical." Thus, a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.

To inform and assist DDs in reporting instances of suspected money laundering, terrorist financing, and fraud, FinCEN issues advisories and guidance containing examples of "red flags." In order to assist law enforcement in its efforts to target these activities, FinCEN requests that DDs check the appropriate box(es) in the Suspicious Activity Information section and include certain key terms in the narrative section of the SAR. The advisories and guidance can be found on FinCEN Web site.[232]

By their nature, SAR narratives are subjective, and examiners generally should not criticize the DD's interpretation of the facts. Nevertheless, DDs should ensure that SAR narratives are complete, thoroughly describe the extent and nature of the suspicious activity, and are included

---

[230] *Id.*

[231] For suspicious activity related to terrorist activity, institutions may also call FinCEN's Financial Institution's terrorist hot line's toll-free number (866) 556-3974 (seven days a week, 24 hours a day) to further facilitate the immediate transmittal of relevant information to the appropriate authorities.

[232] For more information, refer to SAR Advisory Key Terms on the FinCEN Web site.

within the SAR. Furthermore, DDs should develop and implement processes and procedures for conducting quality control on SARs before they are filed. The BSAR accepts a single, Microsoft Excel-compatible comma separated value (csv) file no larger than one (1) megabyte as an attachment as part of the report. This capability allows a DD to include transactional data such as specific financial transactions and funds transfers or other analytics that are more readable or usable in this format than it would be if otherwise included in the narrative. Such an attachment is be considered a part of the narrative and is not considered to be a substitute for the narrative.

For example, narratives should not simply state "see attachment" if the DD included a csv attachment. As with other information that may be prepared in connection with the filing of a SAR, an attachment is considered supporting documentation and should be treated as confidential to the extent that it indicates the existence of a SAR.

More specific guidance is available in Appendix L ("SAR Quality Guidance") of the FFIEC AML Manual to assist DDs in writing, and assist examiners in evaluating, SAR narratives.[233]

Notifying Board of Directors of SAR Filings

DDs are required by SAR regulations to notify the board of directors or an appropriate board committee that SARs have been filed. However, the regulations do not mandate a particular notification format and DDs should have flexibility in structuring their format. Therefore, DDs may, but are not required to, provide actual copies of SARs to the board of directors or a board committee. Alternatively, DDs may opt to provide summaries, tables of SARs filed for specific violation types, or other forms of notification. Regardless of the notification format used by the DD, management should provide sufficient information on its SAR filings to the board of directors or an appropriate committee in order to fulfill its fiduciary duties, while being mindful of the confidential nature of the SAR.[234]

Record Retention and Supporting Documentation

DDs must retain copies of SARs and supporting documentation for five years from the date of filing the SAR. The DD can retain copies in paper or electronic format. Additionally, DDs must provide all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or federal banking agency. "Supporting documentation" refers to all

[233] Guidance to assist DDs in filing SARs can be found in the "FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Requirements," Version 1.2 (Release Date October 2012). Other guidance available from FinCEN includes "Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting" (October 2007).

[234] As noted in the Bank Secrecy Act Advisory Group's *The SAR Activity Review – Trends, Tips & Issues*, Issue 2, (June 2001), "In the rare instance when suspicious activity is related to an individual in the organization, such as the president or one of the members of the board of directors, the established policy that would require notification of a SAR filing to such an individual should not be followed. Deviations to established policies and procedures so as to avoid notification of a SAR filing to a subject of the SAR should be documented and appropriate uninvolved senior organizational personnel should be so advised."

documents or records that assisted a DD in making the determination that certain activity required a SAR filing. No legal process is required for disclosure of supporting documentation to FinCEN or an appropriate law enforcement or federal banking agency.[235]

Prohibition of SAR Disclosure

No DD, and no director, officer, employee, or agent of a DD that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported whether the transaction is fiat-based or digital asset-based. A SAR and any information that would reveal the existence of a SAR, are confidential, except as is necessary to fulfill BSA obligations and responsibilities. For example, the existence or even the non-existence of a SAR must be kept confidential, as well as the information contained in the SAR to the extent that the information would reveal the existence of a SAR.[236] Furthermore, FinCEN and the Department/federal banking regulators take the position that a DD's internal controls for the filing of SARs should minimize the risks of disclosure.

A DD or its agent may reveal the existence of a SAR to fulfill responsibilities consistent with the BSA, provided no person involved in a suspicious transaction is notified that the transaction has been reported. The underlying facts, transactions, and supporting documents of a SAR may be disclosed to another financial institution for the preparation of a joint SAR, or in connection with certain employment references or termination notices to the full extent authorized in 31 USC 5318(g)(2)(B). The sharing of a SAR by a DD or its agent with certain permissible entities within the DD's corporate organizational structure for purposes consistent with Title II of the Bank Secrecy Act is also allowed.

Any person subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR, except when such disclosure is requested by FinCEN or an appropriate law enforcement[237] or a banking regulator, shall decline to produce the SAR or to provide any information that would disclose that a SAR has been prepared or filed, citing 31 CFR 1020.320(e) and 31 USC 5318(g)(2)(A)(i). FinCEN, the DD's federal banking agency when applicable, and the Department should be notified of any such request and of the DD's response.

---

[235] Refer to *Suspicious Activity Report Supporting Documentation* (June 2007).

[236] FinCEN and the OCC issued final rules amending the confidentiality provisions of suspicious activity reports. The rules clarify how, when, and to whom SAR information, and the existence of a SAR may be disclosed. Refer to 75 Fed. Reg. 75576 (December 2010) (OCC) and 75 Fed. Reg. R 75593 (December 2010) (FinCEN).

[237] Examples of agencies to which a SAR or the information contained therein could be provided include: the criminal investigative services of the armed forces; the Bureau of Alcohol, Tobacco, and Firearms; an attorney general, district attorney, or state's attorney at the state or local level; the Drug Enforcement Administration; the Federal Bureau of Investigation; the Internal Revenue Service or tax enforcement agencies at the state level; the Office of Foreign Assets Control; a state or local police department; a United States Attorney's Office; Immigration and Customs Enforcement; the U.S. Postal Inspection Service; and the U.S. Secret Service. For additional information, refer to Bank Secrecy Act Advisory Group, "Section 5 – Issues and Guidance," *The SAR Activity Review – Trends, Tips & Issues,* Issue 9, page 44 (October 2005) on the FinCEN Web site.

Examiners should follow their respective agency's protocol on discovery of the improper disclosure of a SAR. Examiners also should ensure the DD has notified the Department and FinCEN of the improper disclosure. Department examiners should follow internal escalation processes in the event of such disclosures for further determination and actions.

Sharing SARs With Head Offices, Controlling Companies, and Certain U.S. Affiliates

Previously issued guidance clarified that sharing of a SAR or, more broadly, any information that would reveal the existence of a SAR, with a head office or controlling company (including overseas) promotes compliance with the applicable requirements of the BSA by enabling the head office or controlling company to discharge its oversight responsibilities with respect to enterprise-wide risk management, including oversight of a DD's compliance with applicable laws and regulations.[238]

A controlling company as defined in the guidance includes:

- A bank holding company (BHC), as defined in section 2 of the BHC Act.
- A savings and loan holding company, as defined in section 10(a) of the Home Owners' Loan Act.
- A company having the power, directly or indirectly, to direct the management policies of an industrial loan company or a parent company or to vote 25 percent or more of any class of voting shares of an industrial loan company or parent company.

The guidance confirms that:

- A U.S. branch or agency of a foreign DD may share a SAR with its head office outside the United States.
- A U.S. DD may share a SAR with controlling companies whether domestic or foreign.

In addition, a DD that has filed a SAR may share the SAR, or any information that would reveal the existence of the SAR, with an affiliate provided the affiliate is subject to a SAR regulation.[239] An affiliate is defined as any company under common control with, or controlled by, that depository. Under "common control'' means that another company:

- Directly or indirectly or acting through one or more other persons owns, controls, or has the power to vote 25 percent or more of any class of the voting securities of the company and the depository; or
- Controls in any manner the election of a majority of the directors or trustees of the company and the depository.

[238] FinCEN, Federal Reserve, FDIC, OCC, and OTS, "Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies" (January 2006).

[239] FinCEN, "Sharing Suspicious Activity Reports by Depository Institutions with Certain U.S. Affiliates" (FIN-2010-G006) (November 2010).

Controlled by means that the depository:

- Directly or indirectly has the power to vote 25 percent or more of any class of the voting securities of the company; or
- Controls in any manner the election of a majority of the directors or trustees of the company. See 12 USC 1841(a)(2).

Because foreign branches of U.S. DDs are regarded as foreign DDs for the purposes of the BSA, they are affiliates that are not subject to a SAR regulation. Accordingly, a U.S. DD that has filed a SAR may not share the SAR, or any information that would reveal the existence of the SAR, with its foreign branches.

DDs should maintain appropriate arrangements with head offices, controlling companies, and affiliates to protect the confidentiality of SARs. The DD should have policies and procedures in place to protect the confidentiality of the SAR as part of their internal controls.

3.3.1. Suspicious Activity Reporting – Examination Procedures

Objective. *Assess the DD's policies, procedures, and processes, and overall compliance with statutory and regulatory requirements for monitoring, detecting, and reporting suspicious activities.*

Procedure	Comments
Initially, examiners may elect to "map out" the process the DD follows to monitor for, identify, research, and report suspicious activities. Once the examiner has an understanding of the process, the examiner should follow an alert through the entire process.	
Identification of Unusual Activity	
1. Review the DD's policies, procedures, and processes for identifying, researching, and reporting suspicious activity for all fiat-based and digital asset activity. Determine whether they include the following: • Lines of communication for the referral of unusual activity to appropriate personnel. • Designation of individual(s) responsible for identifying, researching, and reporting suspicious activities. • Monitoring systems used to identify unusual activity (including the use of both traditional monitoring systems and digital asset analytics systems) for each product or service that the DD offers. As part of this review, Department examiners may consider how the DD incorporates metrics or findings from each key suspicious activity monitoring component to create a responsive monitoring process. Additionally, examiners should assess the manner in which the DD's digital asset analytics platform is integrated with other transaction monitoring or other related systems, including measures designed to ensure data quality, alert triggers, and potential gaps. • Procedures for reviewing and evaluating the transaction activity of subjects	

Procedure	Comments
included in law enforcement requests (e.g., grand jury subpoenas, section 314(a) requests, or National Security Letters (NSLs)) for suspicious activity. NSLs are highly confidential documents; as such, examiners will not review or sample specific NSLs. Instead, examiners should evaluate the policies, procedures, and processes for: ▪ Responding to NSLs. ▪ Evaluating the account of the target for suspicious activity. ▪ Filing SARs, if necessary. ▪ Handling account closures. ▪ Considering and including digital asset-specific nuances, information, and risks.	
2. Review the DD's monitoring systems and how the system(s) fits into the DD's overall suspicious activity monitoring and reporting process. Complete the appropriate examination procedures that follow. When evaluating the effectiveness of the DD's monitoring systems, examiners should consider the DD's overall risk profile (higher-risk products, services, customers and counterparties, entities, distribution channels, and geographic locations), volume of transactions, and adequacy of staffing. As part of the risk profile review, Department examiners should assess the DD's overall identified AML/CFT and OFAC typologies, corresponding manual or automated controls, and determine whether the DD has sufficient coverage.[240]	
3. Review the DD's digital asset analytics and how the AML/CFT and OFAC system(s) fits into the DD's overall suspicious activity	

[240] For example, Department examiners may assess the number of alerts generated or SARs filed based on the DD's identified AML/CFT and OFAC typologies.

Procedure	Comments
monitoring and reporting process. When evaluating the effectiveness of the DD's analytics, examiners should consider the DD's overall risk profile (higher-risk products, services, customers and counterparties, entities, and geographic locations), volume of transactions, and adequacy of staffing. For example, evaluate whether the DD has controls/processes in place to identify transactions involving higher risk wallet addresses. To the degree that the DD outsources transaction monitoring of on-chain activity, assess whether the DD has clearly documented policies, processes, and procedures clarifying how the blockchain analytics activity integrates into its overall control framework.	
Transaction (Manual Transaction) Monitoring	
4. Review the DD's transaction monitoring reports, including whether there is a written data governance program in place for AML/CFT and OFAC/sanctions-related MIS that feeds into Transaction Monitoring reports. Determine whether the reports capture all areas that pose money laundering and terrorist financing and OFAC risks based on the DD's risk profile. This review should include both fiat-based AML/CFT and OFAC typologies and digital asset-specific typologies. Examples of these reports for fiat-based activities include: currency activity reports, funds transfer reports, monetary instrument sales reports, ATM transaction reports, large item reports, significant balance change reports, nonsufficient funds (NSF) reports, and nonresident alien (NRA) reports. Examples of these reports for digital assets-based activities include virtual currency funds	

Procedure	Comments
transfers reports and digital asset analytics reports.	
5. Determine whether the DD's transaction monitoring systems use reasonable filtering criteria whose programming has been independently verified. This review should include the DD's approach for fiat-based typologies addressed through transaction and surveillance monitoring systems as well as digital assets-specific typologies.[241] For example, for each virtual currency that the DD on-ramps or off-ramps, determine what measures are in place for the DD to identify customers attempting to structure transactions. Determine whether the monitoring systems generate accurate reports at a reasonable frequency.	
Surveillance (Automated Accounting) Monitoring	
6. Identify the types of customers, products, distribution channels, and services that are included within the surveillance monitoring system.	
7. Identify the system's methodology for establishing and applying expected activity or profile filtering criteria for each customer, and as applicable counterparty relationships, and for generating monitoring reports.[242] Determine whether the system's filtering criteria are reasonable, including via conducting regular model validation.	

[241] Rules or scenarios may also consider how the DD has identified appropriate typologies for their supported products and services and specific risk profile, how these typologies are addressed through manual or automated scenarios with appropriate thresholds. In each instance, the Department examiner should evaluate what rules the DD has in place (whether through traditional automated transaction monitoring systems or digital asset analytics) to address identified AML/CFT and OFAC risk typologies.

[242] For example, Department examiners may review the ability of the DD to generate a unique customer profile that accounts for all activity (including fiat-based and digital assets products and services) to inform decision-making for filing of a SAR.

Procedure	Comments
Where the DD relies on third-parties to augment its transaction monitoring, determine whether the DD has applied sound risk management practices to third-party oversight and model implementation, including obtaining sufficient information from the third party to understand how the model operates and performs, ensuring that it is working as expected, and tailoring its use to the unique risk profile of the DD.	
8. Determine whether the programming of the methodology has been independently validated by individuals with sufficient expertise and an appropriate level of independence from the model's development and implementation.	
9. Determine whether controls ensure limited access to the monitoring system and sufficient oversight of assumption changes for each fiat-based and digital assets system.	
Managing Alerts	
10. Determine whether the DD has policies, procedures, and processes to ensure the timely generation of, review of, and response to reports used to identify unusual activities from each manual and automated source.	
11. Determine whether policies, procedures, and processes require appropriate research when monitoring reports identify unusual activity.[243]	
12. Evaluate the DD's policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating	

[243] Examiners could consider open-source reviews and negative news screening among other due diligence measures, as well as appropriate escalation and review processes in place taking account of the specific digital assets and digital assets products that the DD offers.

Procedure	Comments
unusual activity. The process should ensure that all applicable information (e.g., criminal subpoenas, NSLs, and section 314(a) requests and 314(b) requests, if applicable) is effectively evaluated. As part of this review, determine what governance and internal reporting are in place around alert reviews (e.g., alert aging and escalations) with appropriate management oversight.	
13. Verify that staffing levels are sufficient to review reports and alerts and investigate items, and that staff possess the requisite experience level and proper investigatory tools. The volume of system alerts and investigations should not be tailored solely to meet existing staffing levels.	
14. Determine whether the DD's SAR decision process appropriately considers all available CDD and EDD information.	
SAR Decision Making	
15. Determine whether the DD's policies, procedures, and processes include procedures for: • Documenting decisions not to file a SAR. • Escalating issues identified as the result of repeat SAR filings on accounts. • Considering closing accounts as a result of continuous suspicious activity. For each consideration, evaluate what metrics the DD currently has in place to track and escalate alert and SAR-related decisions (e.g., number of	
SAR Completion and Filing	
15. Determine whether the DD's policies, procedures, and processes provide for: • Completing, filing, and retaining SARs and their supporting documentation.	

Procedure	Comments
• Reporting SARs to the board of directors, or a committee thereof, and informing senior management, as well as roles and responsibilities for each type of SAR filing. • Sharing SARs with head offices and controlling companies, as necessary. • Conducting quality control on SAR narratives before they are filed.	

Transaction Testing

Transaction testing of suspicious activity monitoring systems and reporting processes is intended to determine whether the DD's policies, procedures, and processes are adequate and effectively implemented. Examiners should document the factors they used to select samples and should maintain a list of the accounts sampled. The size and the sample should be based on the following:

- Weaknesses in the account monitoring systems.
- The DD's overall AML/CFT risk profile (e.g., number and type of higher-risk products, services, customers, entities including counterparties, distribution channels, and geographies).
- Quality and extent of review by audit or independent parties.
- Prior examination findings.
- Recent mergers, acquisitions, or other significant organizational changes.
- Conclusions or questions from the review of the DD's SARs.

Refer to Appendix O in the FFIEC AML Manual ("Examiner Tools for Transaction Testing") for additional guidance on examiner requests in the event that a DD does not have preset filtering reports for currency transaction reporting and the identification of suspicious currency transactions (e.g., for a specific digital asset).

16. On the basis of a risk assessment, prior examination reports, and a review of the DD's audit findings, sample specific customer accounts to review the following: • Suspicious activity monitoring reports. • CTR download information. • Higher-risk banking operations (products, services, customers and counterparties, entities, distribution channels, and geographies). • Customer activity. • Subpoenas received by the DD.	

Procedure	Comments
• Decisions not to file a SAR.	
17. For the customers selected previously, obtain the following information, if applicable: • CIP and account-opening documentation. • CDD documentation. • Two to three months of account statements covering the total customer relationship and showing all transactions. • Sample items posted against the account (e.g., copies of checks deposited and written, debit or credit tickets, and funds transfer beneficiaries and originators). • Other relevant information, such as loan files and correspondence.	
18. Review the selected accounts for unusual activity. If the examiner identifies unusual activity, review customer information for indications that the activity is typical for the customer (i.e., the sort of activity in which the customer is normally expected to engage). When reviewing for unusual activity, consider the following: • For business customers, whether the activity is consistent with CDD information (e.g., type of business, size, location, and target market).	
19. Determine whether the transaction or surveillance suspicious activity monitoring system detected the activity that the examiner identified as unusual.	
20. For transactions identified as unusual, discuss the transactions with management. Determine whether the account officer demonstrates knowledge of the customer and the unusual transactions. After examining the available facts, determine whether management knows of a reasonable explanation for the transactions.	

Procedure	Comments
21. Determine whether the DD has failed to identify any reportable suspicious activity for either fiat-based or digital asset activity.	
22. From the results of the sample, determine whether the transaction or surveillance suspicious activity monitoring system effectively detects unusual or suspicious activity. Identify the underlying cause of any deficiencies in the monitoring systems (e.g., inappropriate filters, insufficient risk assessment, or inadequate decision-making).	
23. On the basis of a risk assessment, periodic digital asset transaction testing, prior examination reports, and a review of the DD's audit findings, select a sample of management's decisions to determine the following: • Whether management decisions to file or not file a SAR are supported and reasonable. • Whether documentation is adequate. • Whether the decision process is completed, and SARs are filed in a timely manner.	
24. On the basis of a risk assessment, prior examination reports, and a review of the DD's audit findings, sample the SARs downloaded from the BSA reporting database or the DD's internal SAR records. Review the quality of SAR content to assess the following: • SARs contain accurate information. • SAR narratives are complete and thorough, and clearly explain why the activity is suspicious (i.e., the SAR narrative should not simply state "see attachment" if the DD included a csv file).	
25. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of	

Procedure	Comments
policies, procedures, and processes to meet regulatory requirements associated with monitoring, detecting, and reporting suspicious activity.	

3.4. Currency Transaction Reporting

Objective. *Assess the DD's compliance with the BSA regulatory requirements for currency transaction reporting.*

Regulatory Requirements for Currency Transaction Reporting

This section outlines the regulatory requirements for DDs found in 31 CFR Chapter X regarding reports of transactions in currency. Specifically, this section covers:

- 31 CFR 1010.310
- 31 CFR 1010.311
- 31 CFR 1010.312
- 31 CFR 1010.313
- 31 CFR 1010.314

Filing Obligations

A DD must electronically file a Currency Transaction Report (CTR) for each transaction in currency (deposit, withdrawal, exchange of currency, or other payment or transfer) of more than $10,000 by, through, or to the DD. For digital assets, CTR requirements may apply during fiat on and off ramping. Further, in a proposed rule published in January 2021, FinCEN recommended extending transaction reporting requirements to certain transactions involving digital assets with legal tender status. Such VCTRs would be submitted on a Value Transaction Report form similar to the existing FinCEN CTR form.[244] These currency transactions need not be reported if they involve "exempt persons," a group which can include commercial customers meeting specific criteria for exemption. Refer to the *Transactions of Exempt Persons* section for more information.

Identification Required

A DD must verify and record the name and address of the individual presenting a transaction, as well as record the identity, account number, and Social Security or taxpayer identification number, if any, of any person or entity on whose behalf such a transaction is conducted. Verification of the identity of an individual who indicates that he or she is an alien or is not a resident of the United States must be made by passport, alien identification card, or other official document evidencing nationality or residence (e.g., a provincial driver's license with indication of home address). Verification of identity in any other case must be made through a document, other than a DD signature card, that is normally acceptable as a means of identification when cashing checks for nondepositors (e.g., a driver's license). A DD signature card may be relied upon only if it was issued after documents establishing the identity of the individual were examined and notation of

[244] FinCEN Proposed Rule, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" (January 2021).

the specific information was made on the signature card. In each instance, the specific identifying information (e.g., the driver's license number) used in verifying the identity of the customer must be recorded on the report. The mere notation of "known customer" or "DD signature card on file" on the report is prohibited.

Aggregation of Currency Transactions

For the purposes of currency reporting requirements, a DD includes all of its domestic branch offices and, therefore, branch office transactions must be aggregated. Multiple currency transactions resulting in either cash in or cash out totaling more than $10,000 during any one business day must be treated as a single transaction, if the DD has knowledge that they are conducted by or on behalf of any person. Deposits made at night or over a weekend or holiday must be treated as if received on the next business day following the deposit. To comply with regulatory requirements, management must ensure that systems or practices appropriately aggregate currency transactions throughout the DD and report currency transactions subject to the BSA requirement to file CTRs.

Types of currency transactions subject to reporting requirements individually or by aggregation include, but are not limited to: deposits and withdrawals, automated teller machine (ATM) transactions (including virtual currency ATMs or kiosks), denomination exchanges, loan payments, currency transactions used to fund individual retirement accounts (IRAs), purchases of certificates of deposit, funds transfers paid for in currency, monetary instrument purchases, certain transactions involving armored car services, and currency to or from prepaid access.

In cases where multiple businesses share a common owner, FinCEN guidance states that the presumption is that separately incorporated entities are independent persons. This FinCEN guidance indicates that the currency transactions of separately incorporated businesses should not automatically be aggregated as being on behalf of any one person simply because those businesses are owned by the same person. It is up to the DD to determine, based on information obtained in the ordinary course of business, whether multiple businesses that share a common owner are, in fact, being operated independently depending on all the facts and circumstances. Consistent with this FinCEN guidance, if the DD determines that the businesses are independent, then the common ownership does not require aggregation of the separate transactions of these businesses.

However, if the DD determines that these businesses (or one or more of the businesses and the private accounts of the owner) are not operating separately or independently of one another or their common owner (e.g., the businesses are staffed by the same employees and are located at the same address, the DD accounts of one business are repeatedly used to pay the expenses of another business, or the business DD accounts are repeatedly used to pay the personal expenses of the owner), the DD may determine that aggregating the businesses' transactions is appropriate because the transactions were made on behalf of a single person. Consistent with this FinCEN guidance, once the DD determines that the businesses are not independent of each other or of their common owner, then the transactions of these businesses should be aggregated going forward.

There are other BSA requirements that may aid DDs in determining when transactions are "by or on behalf of" the same person, such as the requirement to identify the beneficial owners of legal entity customers. To the extent this beneficial ownership information helps the DD determine that

certain transactions had no apparent purpose other than to avoid triggering a CTR filing, the DD would need to consider whether filing a suspicious activity report (SAR) would be appropriate. Refer to the *Beneficial Ownership Requirements for Legal Entity Customers* section for more information.

Structured Transactions – CTR Requirements

Structuring transactions occurs when a person, acting alone or in conjunction with, or on behalf of, other persons, conducts or attempts to conduct one or more transactions in currency, in any amount, at one or more financial institutions, on one or more days, in any manner, for the purpose of evading the CTR requirements.

Under the BSA, no person shall, for the purpose of evading a CTR reporting requirement:

- Cause or attempt to cause a DD to fail to file a CTR.
- Cause or attempt to cause a DD to file a CTR that contains a material omission or misstatement of fact.
- Structure, assist in structuring, or attempt to structure any transaction with one or more domestic financial institutions.

Refer to *Appendix G: Structuring* of the FFIEC Manual for additional information. When a DD suspects that a person is structuring transactions to evade CTR filing, it must file a SAR. Additionally, evading BSA reporting and recordkeeping requirements can result in civil and criminal penalties under the BSA.

Filing and Record Retention

All CTRs must be filed through FinCEN's BSA E-Filing System. Certain fields in the CTR are marked as "critical" for technical filing purposes; this means the BSA E-Filing System does not accept filings in which these fields are left blank. For these items, FinCEN filing instructions state that the DD must either provide the requested information or check "unknown." FinCEN expects that DDs will provide the most complete filing information available, consistent with existing regulatory expectations, regardless of whether the individual fields are deemed critical for technical filing purposes. If the DD receives correspondence from FinCEN identifying data quality errors, it should follow any required actions that FinCEN outlines in the correspondence. FinCEN has also issued several administrative rulings and other guidance on filing and completing CTRs.

A completed CTR must be electronically filed with FinCEN within 15 calendar days after the date of the transaction. The DD must retain copies of CTRs for five years from the date of the report. The DD may retain copies in either electronic format or paper copies.

FinCEN's BSA E-Filing System allows for tracking of filings. Users will receive acknowledgement notifications and other correspondence from FinCEN through the system regarding their filings. Examiners should consider reviewing correspondence from FinCEN's BSA E-Filing System to aid in their assessment of the DD's reporting of currency transactions.

CTR Backfiling and Amendment

If the DD becomes aware, either through self-identification or through an examination, that it has failed to file CTRs on reportable transactions, or filed CTRs with errors, the DD must begin complying with CTR requirements. The DD may contact FinCEN's Resource Center to request a determination on whether to backfile unreported transactions or amend CTRs filed with errors. In most cases, the DD can submit late CTRs and/or amended CTRs without the need to contact FinCEN for a backfiling or amendment determination. FinCEN has indicated, however, that in certain situations, the DD should consider contacting FinCEN (for example, if the DD is instructed to by its regulator, if it is unclear whether the circumstances require backfiling or amending CTRs, or if the DD wants to request regulatory relief from submitting some or all of the CTRs). Once FinCEN provides a backfiling or amendment determination, the DD should follow the instructions for backfiling or amending CTRs on FinCEN's website.

Examiner Assessment of the CTR Process

Examiners should assess the adequacy of the DD's policies, procedures, and processes (internal controls) related to the DD's reporting of currency transactions. Specifically, examiners should determine whether these internal controls are designed to mitigate and manage ML/TF and other illicit financial activity risks and comply with CTR requirements. In addition to reviewing correspondence from FinCEN's BSA E-Filing System, examiners may review other information, such as recent independent testing or audit reports, to aid in their assessment of the DD's reporting of currency transactions.

Examiners should also consider general internal controls concepts, such as dual controls, segregation of duties, and management approval for certain actions, as they relate to the DD's reporting of currency transactions. For example, employees who complete CTRs generally should not also be responsible for the decision to file the reports. Other internal controls may include BSA compliance officer or other senior management approval for staff actions that override currency aggregation systems and review of exception reports for those overrides.

Given the rise of bulk cash smuggling and other crimes involving both fiat and digital assets (e.g., through the use of virtual currency kiosks or "ATMs"),[245] examiners should also evaluate whether the DD has appropriate controls in place for the monitoring and reporting of such activity and transactions. Specifically, in the case that the DD is an owner or operator of a virtual currency ATM, examiners should assess whether CTR requirements are strictly followed and whether controls are in place to closely monitor daily, weekly, and monthly limits.

Examiners should determine whether the DD's internal controls for reporting of currency transactions are designed to assure ongoing compliance with CTR requirements and are commensurate with the DD's size or complexity and organizational structure. More information

[245] U.S. Treasury, "National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing" (March 2022).

can be found in the *Assessing the AML/CFT Compliance Program - AML/CFT Internal Controls* section of this Manual.

3.4.1. Currency Transaction Reporting Examination and Testing Procedures

Objective. *Assess the DD's compliance with BSA regulatory requirements for the reporting of currency transactions.*

Procedure	Comments
1. Review the DD's policies, procedures, and processes that address the preparation, filing, and retention of CTRs (including fiat on and off ramping and virtual CTR requirements associated with digital assets transactions where applicable, pending proposed rule implementation). Determine whether the DD adequately addresses the requirements for preparing, filing, and retaining CTRs.	
2. Assess whether the DD conducts transactions that qualify for CTRs; if yes, determine whether the DD has appropriate policies, procedures, and processes in place to identify transactions that would result in a CTR, how to file the CTR, and applicable recordkeeping requirements.	
3. Review correspondence that the DD has electronically received from FinCEN's BSA E-Filing System. Determine the significance of any errors reported by FinCEN and whether management has taken corrective action, when necessary.	
4. Review the information technology sources, systems, and processes the DD uses to identify transactions that may be required to be reported in a CTR. Determine whether the DD appropriately	

Procedure	Comments
aggregates currency transactions, including throughout DD branch offices.	
5. Determine whether the DD's internal controls are designed to assure ongoing compliance with CTR requirements and are commensurate with the DD's size or complexity and organizational structure. This may include reviewing processes for overriding currency aggregation systems.	
6. Determine whether the DD allows for any fiat and/or traditional banking activities, products, and services (including virtual asset kiosks or "ATMs"). If the DD allows for such activity, evaluate the controls it has in place specifically for the monitoring and reporting of these transactions.	
7. Select a sample of filed CTRs (electronic format or paper copies) to determine whether: • CTRs are filed in accordance with FinCEN instructions for currency transactions identified by the information technology sources, systems, and processes the DD uses. • CTRs are filed within 15 calendar days after the date of the transaction(s). • CTRs filed contain accurate and complete information. Determine whether management has taken corrective action when errors are identified internally or by FinCEN's BSA E-Filing System. • Any discrepancies exist between the DD's records of CTRs and the CTRs reflected in the BSA reporting database.	

Procedure	Comments
• The DD retains copies (electronic format or paper copies) of CTRs for five years from the date of the report.	
8. On the basis of examination and testing procedures completed, form a conclusion about the adequacy of policies, procedures, and processes the DD has developed to meet BSA regulatory requirements associated with reporting of currency transactions.	

3.5. New Products, Processes, and Technologies – Overview

Objective. *Assess the DD's policies, procedures, and processes related to the identification, assessment, and mitigation of money laundering and terrorist financing risks associated with new and emerging products, practices, and technologies.*

As the digital asset and financial technology environment evolves rapidly, new products, practices, and technologies will emerge. These developments will present new opportunities, but DDs must also identify, assess, and mitigate new risks that arise through the use of such new products, practices, and technologies, as well as evaluate the impact that new technologies (e.g., use of a new distribution channel) pose on both new and existing products and practices.

DDs should assess the money laundering, terrorist financing, and OFAC compliance risks, in addition to other non-financial crime related risks (e.g., credit, operational, market, reputational, strategic) associated with new products, practices, and technologies.[246] AML/CFT and OFAC-based product risk assessments should be performed prior to the launch of the new product, practice, or technology, with approvals by appropriate executive officers and the board of directors.[247] As warranted, the DD should conduct testing to assess that the new activity complies with AML/CFT and OFAC requirements (including, among others, the ability to maintain auditable records for transactions associated with newly launched product and verifiable internal controls relating to the activity). DDs should have controls, including formalized policies and procedures for new product decisions, with a special focus on new coin or digital asset approvals, including processes for digital asset due diligence and criteria that include AML/CFT and OFAC considerations for accepting or rejecting coins/assets (such considerations may include the level of blockchain analytics coverage of the proposed digital asset, whether the asset has anonymity-enhancing features or other inherent characteristics that are attractive to or have been known to be exploited by illicit actors, the common use cases associated with the asset and whether these known use cases pose unique AML/CFT and OFAC risks, as well as negative news on the founding team associated with the proposed digital asset). The Department expects DDs to document their decision-making/rationale for permissible and rejected digital assets. Where a DD deems a digital asset as higher risk from a AML/CFT and/or OFAC perspective and determines that the digital asset is permissible, the DD should formally document the specific controls it implements to mitigate the risks associated with the higher risk digital asset (such as restricting digital assets with anonymity enhancing features to support only unshielded transactions).

---

[246] See "5-2 A payment service provider's assessment of ML/TF risks in relation to new products, practices and technologies is separate from, and in addition to, the payment service provider's assessment of other risks such as credit risks, operational risks or market risks" from the Monetary Authority of Singapore's "Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism" (March 2020).

[247] See Recommendation 15, "Guidance For a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," (June 2019).

DDs should have documented evaluation measures to ensure AML/CFT and OFAC compliance prior to launching a new product or introducing a new technology (e.g., new product/technology approval policy or procedure, new product/technology review and approval committee with participation from the AML/CFT and OFAC compliance team, etc.). Criteria to address ML/TF and sanctions evasion should, at a minimum, consider the following elements:

- Whether the new product, service, technology, or delivery method promotes anonymity (e.g., AECs), obfuscates transactions, or otherwise challenges an institution's ability to identify appropriately its customers or their counterparties, or implement effective CDD, transaction monitoring, or other AML/CFT measures.
    - However, this element should consider the legitimate uses of technology, including AECs, to guard against asset theft, provide enhanced IT security or provide an additional layer of privacy in the absence of criminal activity which may be desirable for certain individuals subject to identity theft or individuals with a public profile. These legitimate uses should always be grounded in strong customer due diligence, an assessment of the customer's intended uses, the customer's established relationship with the DD, and transaction monitoring. Additionally, a DD may request transaction data and other identifying information to screen privacy coin transactions appropriately;
- Whether the new product, service, technology, or delivery method is susceptible to market manipulation, fraud (e.g., due to market liquidity or volatility), or operational failure that poses unique AML/CFT or OFAC risks;
- Whether the new product, service, or technology creates unique geography risks, including new exposure to high-risk and/or sanctioned jurisdictions; and
- Whether the new product, service, technology, or delivery method is known to be used for illicit purposes, or associated with common illicit typologies associated with digital assets or otherwise.[248]

Further, appropriate steps should be taken to mitigate or eliminate the risks identified with appropriate testing as warranted (e.g., additional CDD measures, limits on usage based on customer type or geography, heightened monitoring standards and record-keeping, or segmentation due diligence and controls).[249] Additionally, new products or related activities should consider potential exposure or involvement of any of the below groups or networks as part of the DD's product risk assessment and mitigation plan.

- Darknet marketplaces;
- Mixers and tumblers;

---

[248] Monetary Authority of Singapore, *Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism* (March 2020).

[249] Bermuda Monetary Authority, "Guidance for AML/ATF Regulated Financial Institutions on Anti-Money Laundering and Anti-Terrorist Financing Notice 2016" (September 2016).

- Privacy wallets;
- Stablecoins;
- Non-fungible tokens;
- Decentralized finance;
- IP addresses in high-risk geographies;
- Unregistered or illicitly operating P2P exchangers;
- Unregistered foreign-located MSBs;
- Unregistered or illicitly operating CVC kiosks;
- Illicit activity leveraging CVC kiosks[250]; and/or
- Gaming and gambling.

As the industry and regulatory supervision continues to evolve, DDs should also demonstrate and document processes to update their new products and new coin assessment processes to address emergent typologies or other groups or networks that pose a higher risk for illicit activity and sanctions evasion.

[250] See "Red Flag Indicators of the Abuse of Virtual Currencies," pp. 7-10 of PDF (May 2019).

3.5.1. New Products, Practices, and Technologies for DDs – Examination Procedures

Objective. *Assess the adequacy and completeness of the DD's ML/TF risk assessments for new products, practices, and technologies. Confirm required risks have been considered and mitigated, and confirm that all products have undergone the appropriate ML/TF risk assessment.*

Procedure	Comments
If this is a standalone new products examination, refer to the core examination procedures, "Scoping and Planning," for comprehensive guidance on the AML/CFT examination scope. In such instances, the new products examination may need to cover additional areas, including training, the BSA compliance officer, independent review, and follow-up items.	
1. Review the policies, procedures, and processes related to the assessment and mitigation of the ML/TF risks posed by new products, practices, and technologies (e.g., new product/technology approval policy or procedure, new product/technology review and approval committee with participation from the AML/CFT and OFAC compliance team, etc.). Evaluate the adequacy of the policies, procedures, and processes given the DD's activities and the risks they present. Assess whether the controls are adequate to reasonably protect the DD from money laundering and terrorist financing.	
2. Review the DD's process for identifying when a product, practice, and/or technology should be treated as 'new' (new to the DD) or a new technology is used for an existing or new product or service offering (or new distribution channel).	
3. Review the DD's procedures for gathering additional information about a new product, practice, or technology as it relates to potential anonymity/pseudonymity and potential risk management options.	
4. Based on a review of MIS and internal risk rating factors, determine whether the DD	

Procedure	Comments
effectively identifies and monitors new products, practices, and technologies.	
5. Determine how the DD includes new products, practices, or technologies into AML/CFT systems and other key control processes.	
6. Review the controls and formalized procedures and policies the DD has in place to prevent AECs from being used for ransomware and other illicit purposes. For example, evaluate whether the DD has a coin due diligence policy or procedure that includes which coins/digital assets the DD will support, as well as coin coverage through blockchain analytics providers. Where higher risk digital assets (e.g., AECs) are permissible, determine the DD's specific risk mitigation controls and documented rationale for supporting the asset(s).	
7. Determine what change management controls are in place for updates to products based on emergent industry trends and/or supervisory practices.	

3.6. Digital Asset Analytics – Overview

Objective. *Assess the DD's policies, processes, and procedures related to the use of digital asset analytics to conduct customer due diligence, develop risk profiles, monitor and detect unusual activity associated with digital asset transactions, and conduct transaction tracing to assess source and destination of funds.*

Note: this section does not set forth standards separate from federal AML/CFT and OFAC requirements. However, given the novelty and unique nature of digital assets, it provides a high-level overview of available digital asset analytics processes. Department examiners should review the DD's digital asset analytics capabilities in addition to traditional control processes (including 3.1. Customer Due Diligence, 3.2. Suspicious Activity Reporting, and others as warranted based on the DD's risk profile) to form an overall view.

Digital assets and their supporting infrastructure create novel challenges to traditional approaches to compliance with, and enforcement of, AML/CFT and OFAC requirements.

The ability of owners of virtual currencies and other digital assets (e.g., certain stablecoins) to transfer ownership without the use of a regulated third party (e.g., between unhosted wallets or to and from an un-registered foreign MSB), creates novel issues to implementing an effective AML/CFT and OFAC compliance program. For most types of digital assets, information stored on the public blockchain ledger (or "on-chain") includes certain identifying information, including sender and receiver wallet addresses, timestamp and date of the transaction, the value of the transaction, and certain additional metadata, such as the associated transaction block and any transaction fees paid by the sender.[251] However, this information is generally pseudonymous, with nothing on the face of the transfer enabling a party to tie back the publicly available information to the transaction's originator, beneficiary, or underlying beneficial owners. Moreover, to execute a digital asset transaction, the capture of originator, beneficiary and beneficial owner information is not required nor do there typically exist additional message fields to capture this information. Due to these inherent digital asset features, standard AML and OFAC sanctions compliance control processes, including funds transfer recordkeeping requirements (refer to *3.7. Virtual Currency Funds Transfers Recordkeeping* for additional information) and transaction screening, cannot be readily applied to digital asset activity without material changes.

Notwithstanding these challenges, the immutable nature of the blockchain ledger allows for a historical view of the digital asset's transfers between digital asset wallet addresses (sometimes referred to as "hops"), enabling visibility into the transaction lineage in a way that is not feasible for traditional funds transfers. The Department recognizes that blockchain technology and associated analytics tools enable institutions and law enforcement to trace transactions in

[251] While this characterization is true for many popular digital assets, for certain digital assets with anonymity enhancing features such public data may not be accessible on the blockchain. Depending on the digital asset type, the wallet addresses of the sender, the recipient, and/or the transaction amount may all be shielded and cannot be subsequently unshielded by any party, except in some instances, the sender themselves.

furtherance of anti-money laundering objectives and expects DDs to take advantage of the unique characteristics associated with public blockchains through block explorers and commercial blockchain analytics solutions. These unique characteristics of public blockchains, when coupled with attribution, clustering, and other statistical techniques offered by blockchain analytics providers, allow DDs to augment their digital asset AML/CFT and OFAC compliance controls. Accordingly, blockchain analytics providers can enable DDs to address, in part or in some cases in full, the following AML/CFT and OFAC compliance controls:

- **Customer Due Diligence** – per the FFIEC AML Manual, ongoing customer due diligence includes but is not limited to "obtaining and analyzing sufficient customer information to understand the nature and purposes of customer relationships for the purpose of developing a customer risk profile; and conducting ongoing monitoring to identify and report suspicious transactions, and on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers." The use of blockchain analytics tools can support DDs in their efforts to establish a customer's source of funds and identify high risk transaction activity. Blockchain analytics may also be relevant to correspondent account enhanced due diligence. Per 2021 FATF guidance, digital asset service providers have leveraged blockchain analytics capabilities to aid in compliance with funds transfer recordkeeping requirements[252], where capabilities such as 'know your VASP' tools have enabled digital asset service providers to assess the risks associated with intermediaries of digital asset transactions.
    - **Customer Risk Profile** – DDs are expected to have an understanding of the ML/TF risks of its customers (a "customer risk profile"). The customer's risk profile should address actual or anticipated activity, as well as source and destination of funds and wealth. It should also include geographic location, products and services used, and customer type. For further information, refer to *Section 3.2. Customer Risk Profile*. Intelligence gathered from initial digital asset provenance analysis and ongoing transaction monitoring can be used by DDs to build and adapt the customer's profile.
- **Suspicious Activity Monitoring** – per the FFIEC AML Manual, "Appropriate policies, procedures, and processes should be in place to monitor and identify unusual activity. The sophistication of monitoring systems should be dictated by the [DD's] risk profile, with particular emphasis on the composition of higher-risk products, services, customers, entities, and geographies." The use of blockchain analytics tools enables DDs to identify unusual on-chain activity and funds flows, including interactions with high-risk entities (such as darknet markets, unregistered exchanges, mixers/tumblers, sanctioned parties, ransomware providers, etc.), and transaction activity consistent with common digital asset money laundering techniques/typologies (such as chain peeling and chain-hopping).
- **Sanctions Screening** – per the FFIEC AML Manual, the "[DD's] policies, procedures, and processes should address how the [DD] will identify and review transactions and accounts for possible OFAC violations" and have processes for "timely updating of the

[252] FATF, "Second 12 Month Review of Revised FATF Standards - Virtual Assets and VASPs" (July 2021).

lists of sanctioned countries and blocked entities, and individuals, and disseminating such information." A common feature of blockchain analytics tools is the attribution of wallet addresses to addresses that have been designated by OFAC, while clustering methodologies employed by blockchain analytics providers enable the tools to flag additional addresses that are believed to have sanctions exposure based on on-chain interactions. DDs can and should leverage these blockchain analytics capabilities to support their Sanctions Compliance Programs, including sanctions screening, in addition to other technology solutions such as geolocation and IP address blocking, and VPN monitoring.

More recently, an increasing number of digital assets firms are starting to leverage artificial intelligence and "big data" in addition to digital assets analytics for AML and OFAC-related compliance purposes.[253] Further, digital assets firms are implementing real-time transaction screening capabilities by integrating blockchain analytics tools with their custodial/settlement architecture, to further bolster their transaction monitoring and OFAC screening capabilities, thereby enabling preventive rather than solely detective capabilities. Though not an exhaustive list, common control measures executed through blockchain analytics solutions typically include:

- Risk-focused screening of the identity of a digital asset wallet owner;
- Risk profiling of digital asset wallets;
- Transaction tracing for source and destination of funds (including digital asset transaction screening);
- Digital asset transaction monitoring; and
- Digital asset transaction screening.

The Department requires DDs to use digital asset analytics tool(s), either through a third-party provider, or through the development of in-house capabilities. If the DD uses an in-house tool, it is expected to demonstrate through third-party verification that these in-house analytics capabilities are sufficiently accurate and reliable. As noted by FATF, "each [blockchain analytics] company has their own methods, resources, techniques and data which they combine with the data taken from the blockchain. It takes significant time, resources, expertise, and investment for companies to map real-world entities onto wallets… [Further] blockchain analytics is probabilistic and data produced has an inherent level of uncertainty associated with it."[254] Accordingly, the Department expects DDs to have a defensible position on the digital asset analytics tool(s) selected and the level of confidence associated with the tool's methodology. Refer to *3.8. Model Risk Management* for additional information.

Moreover, where DDs outsource key control functions (e.g., screening of customers and counterparties against sanctions lists, PEPs, or adverse news or review of transactions for unusual activity), the DD should have clearly documented policies, processes, and procedures

[253] FATF, "Second 12 Month Review of Revised FATF Standards - Virtual Assets and VASPs" (July 2021).

[254] Ibid

demonstrating how they work with third-party providers. Where the DD relies on a third-party provider to support its digital asset analytics needs, the DD should have clearly documented processes on how the DD integrates with the provider's solution(s), including service level agreements ("SLAs"), contracts, or similar documentation that define the expectations and commitments between the service provider and client—in this case, the DD, on regular solution updates, information sharing, escalations, and the outcomes of any material changes/reviews to the system(s) and associated methodologies.

Digital Asset Wallet Identification

To evaluate transactions for unusual activity, DDs must be able to independently identify transaction counterparties. Additionally, AML/CFT regulations, such as the CIP rule and so-called "travel rule," require DDs to document identifying information about their customers as well as retain records of counterparties to transactions (31 CFR § 1020.410(a)(1)(F)).

Because digital asset wallet addresses are inherently pseudonymous, DDs need tools to help identify and track the identity of the institution(s) associated with a digital asset wallet or the owner of a wallet consistent with customer due diligence and other BSA requirements. Accordingly, Department examiners should assess DDs' policies, processes, and procedures to assess digital asset addresses. Certain analytics providers offer solutions that allow DDs to obtain identifying information (e.g., location of a wallet address on a specific exchange for custodial transactions) that ties directly to the pseudonymous on-chain data on the blockchain ledger. Note that these solutions are in some instances able to identify wallet addresses associated with an institution (e.g., a digital asset exchange) as well as known high-risk wallet addresses (e.g., darknet marketplaces);[255] however, such tools may not be able to identify underlying owners, including ultimate beneficial owners, absent additional information provided by the customer. Moreover, as noted above, there are limitations for any given digital asset analytics provider in terms of the number of wallet address attributions available, including for hosted and unhosted wallets. Accordingly, Department examiners should evaluate the DD's approach to demonstrate how they leverage analytics solutions to form an overall customer profile and screen counterparty information, to the extent reasonably practicable.

Risk Profiling of Digital Asset Wallets

Because digital assets can be 'natively' transferred to or from non-regulated financial institutions, Department examiners should assess the degree to which DDs have policies, processes, and procedures in place to form a risk profile of counterparties. Counterparty risk profiling, or the ability to leverage open-source and proprietary data to develop specific profiles typically with a quantitative score, should clearly define the risk for any entity with whom the DD interacts (e.g.,

[255] Note guidance from the MAS's "Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism" (March 2020): "Payment service providers should utilize data and distributed ledger analytics tools that are commensurate with their risks, as well as size and sophistication of their business, to enhance the detection of suspicious transactions."

VASPs) as well as customers of these entities. Department examiners should assess the DD's processes to assess criteria used to develop risk profiles and scores, with appropriate testing and evidence tying that approach to the DD's own control processes (e.g., via historical SAR filings, findings from independent testing, the most recent risk assessment, or otherwise). The DD's risk profiling methodology should adequately demonstrate the rationale for how scores were developed based on the DD's risk profile, and how the score tied back to the DD's overall risk appetite (e.g., how prohibited activity is appropriately captured through risk profiling), including the approach for hosted versus unhosted wallets.

Transaction Tracing For Source and Destination of Funds

Department examiners should also assess the DD's policies, processes, and procedures for the tracing of transaction activity for each type of digital asset the DD supports, and the flow of funds through the blockchain for any incoming or outgoing activity.

Per FinCEN: "*Blockchain network analytic tools can also tie a targeted bitcoin address and may have information that could potentially help identify beneficial owners. Like other investigative techniques this process requires expenditure of investigative resources to try to follow bitcoin transactions through addresses to a real-world identity, and can involve subpoenas for records at virtual currency businesses."*[256]

Department examiners should assess the DD's approach to leverage virtual asset wallet identification capabilities, publicly available data on the blockchain network, and transaction tracing tools (e.g., distributed ledger technology, like blockchain analytics solutions) to trace digital asset transactions against the DD's risk profile.[257] Transaction tracing examples include (but are not limited to): (1) assessing whether a digital asset has substantial exposure to a high-risk jurisdiction or entity (e.g., darknet market); (2) determining if the transaction(s) was/were processed through a mixer or tumbler, privacy wallet, unregistered peer-to-peer exchanger or decentralized exchange, in what appeared to be an attempt to obfuscate the origin of funds; (3) identifying if the transaction has been associated with scams/ransomware; (4) identifying if the transaction(s) made use of an AEC; and (5) determining if the transaction activity lacked clear business purpose and appeared indicative of attempts to break the chain of custody on its respective public blockchain (i.e., chain-hopping).[258] Additionally, see *3.2. Suspicious Activity Reporting* for considerations around DD coverage relevant to fiat and digital asset-specific typologies as well

[256] Maloney, Drew (FinCEN), Letter from the Department of the Treasury, *Drew Maloney to Ron Wyden* (February 2018).

[257] For example, Department examiners may assess DD documentation to identify that the DD has clear schematics in play to explain its approach for each digital assets type to enable the DD's transaction tracing review process to be reconstructed in an auditable manner.

[258] FinCEN, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" (November 2021).

as *3.8. Model Risk Management* for considerations around configurability of rules against the DD's risk profile.

The DD's documentation should describe case management and escalation processes, with clearly delineated roles and responsibilities across the business and compliance functions, including the DD's approach where there are any doubts about the authenticity of the source of funds.[259,260] For additional Department expectations around source of funds, refer to the *Digital Asset – Customer Due Diligence* section.

Wallet Address Screening. As noted above, in addition to traditional interdiction software used to identify listed entities for sanctions screening (e.g., for wire transfers), certain analytics providers have technology solutions that load certain information, including wallet addresses designated by OFAC, and supplement these wallet address through clustering techniques and data attribution to create probabilistic risk scores as appropriate or ratings identifying related wallet addresses that could be associated with listed persons or a sanctioned jurisdictions. For example, data from blockchain analytics providers points to outsized sanctions risks associated with certain popular stablecoins, emphasizing the importance of blockchain analytics solutions—particularly digital asset wallet screening—to support compliance with U.S. and international sanctions, particularly those related to ransomware.[261] For additional Department expectations around sanctions screening, refer to the *2.4. Assessing the OFAC Compliance Program* section.

Furthermore, DDs should have policies, processes, and procedures in place to assess counterparty exposure for digital assets funds transfers (e.g., beneficiary institutions for outbound transfers)—as an example, "certain vendor products or internally developed tools provide numerical scores or tiered rankings to represent the risk of the counterparty institution, typically based on on-chain transaction data supplemented with other factors such as strength of the institution's AML/CFT Program."[262]

---

[259] Note guidance from ADGM – FSRA, "Guidance – Regulation of Virtual Asset Activities in ADGM" (February 2020), which reads: "The FSRA expects Authorised Persons to develop, implement and maintain effective transactional monitoring systems to determine the origin of a Virtual Asset and to monitor its destination, and to apply strong 'know your transaction' measures which enable Authorised Persons to have complete granular data centric information about the transactions done by a Client."

[260] Note guidance from the MAS's "Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism" (March 2020): "Where the incoming funds in question are [digital payment tokens], a payment service provider should consider if the use of insights from distributed ledger analytics and/or other surveillance tools is necessary to assess the legitimacy of these funds."

[261] Elliptic, "Crypto Addresses Holding NFTs Worth $532k are Among the Latest Sanctioned by OFAC" (November 2021).

[262] Ibid

Digital Assets Transaction Monitoring

Digital asset transaction monitoring systems allow for the ingestion of on-chain transaction data from the blockchain ledger to detect patterns of unusual activity within the DD's customer base.

Consistent with financial institutions' requirements to evaluate transactions for unusual activity, DDs should have policies, processes, and procedures in place to assess the digital asset activity of each of the DD's customers' activities. The processes in place should include adequate coverage of the customer's profiles against applicable typologies and red flags, identify deviations from the profile of the customer's intended purposes from the account, and address other risk considerations as identified (including traditional AML and sanctions typologies such as structuring). Per its 2021 guidance, OFAC emphasizes that firms should consider employing transaction monitoring and investigation tools to "continually review historical information for such addresses or other identifying information to better understand their exposure to sanctions risks and identify sanctions compliance program deficiencies."[263]

These systems should also provide data feeds to enable transaction analysis and the linking of transactions to high-risk of sanctioned countries and criminal activity behavior,[264] as well as assist in identifying transactions involving digital assets addresses and underlying identifying information such as originator and beneficiary associated with sanctioned individuals and/or jurisdictions.[265]

For additional Department expectations, refer to the *3.3. Suspicious Activity Reporting* section.

[263] OFAC, "Sanctions Compliance Guidance for Virtual Currency Industry" (October 2021).

[264] Note guidance from the MAS's Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism" (March 2020): "Payment service providers should utilise data and distributed ledger analytics tools that are commensurate with their risks, as well as size and sophistication of their business, to enhance the detection of suspicious transactions."

[265] New York Department of Financial Services, "Guidance on Use of Blockchain Analytics" (April 2022).

3.6.1. Digital Asset Analytics – Examination Procedures

Objective. *Assess the DD's policies, processes, and procedures related to the use of digital asset analytics to conduct identity verification, develop risk profiles, monitor and detect unusual activity within its digital asset transactions, and conduct transaction tracing to assess source of funds, as appropriate.*

Procedure	Comments
Initially, examiners may elect to "map out" the process the DD follows to monitor for, identify, research, and report suspicious activities. Once the examiner has an understanding of the process, the examiner should follow a representative sample of alerts through the entire process. ***Note:*** *This section assesses use of digital asset analytics service providers. For a review of the controls that such analytics tools are intended to address, Department examiners should review this section in conjunction with the other control sections as appropriate including the 2.4.3. OFAC Internal Controls, 3.2. Customer Due Diligence and 3.3. Suspicious Activity Reporting, and 3.8. Model Risk Management.*	
1. Review the DD's policies, procedures, and processes related to its use of digital asset analytics. Determine whether they include the following: • Appropriate guidance for how analytics solutions integrate into existing controls processes (e.g., service level agreements ("SLAs") or similar documentation that define the expectations and commitments between the service provider and client—in this case, the DD). • Specific digital assets controls (e.g., CDD, customer risk profile, wallet identification, suspicious activity reporting, sanctions screening, and transaction monitoring). • Training of personnel in digital asset analytics techniques and tools.	
2. Request and review a sample of real-time and post-transaction blockchain analytics alerts (where available). Assess the quality of dispositions and associated investigations. On a risk basis, request a "walkthrough" of the investigation	

Procedure	Comments
associated with specific blockchain analytics alert(s).	

3.7. Virtual Currency Funds Transfers Recordkeeping— Overview

Objective. *Assess the DD's compliance with statutory and regulatory requirements for virtual currency funds transfers. This section covers the regulatory requirements as set forth in the BSA. Refer to the expanded sections of this manual for discussions and procedures regarding specific money laundering and OFAC risks for each type of virtual currency funds transfers activity that the DD conducts.*

Note: *this section focuses on funds transfers recordkeeping as it applies to virtual currencies. For traditional fiat-based funds transfers recordkeeping, Department examiners should review the FFIEC AML Manual's Funds Transfers Recordkeeping section.*

Overview of Virtual Currency Funds Transfers Recordkeeping

Funds transfers systems, including transfers of virtual currencies for DDs, enable the instantaneous or near-instantaneous transfer of funds, which in the case of virtual currencies[266] may include originators and beneficiaries that are not regulated financial institutions (i.e., peer-to- peer transactions executed between unhosted wallets). Virtual currency funds transfers contain certain identifying information; however, such information does not include personally identifiable information, such as the names and physical/mailing addresses of originators and beneficiaries, which creates additional challenges for recordkeeping requirements (refer to *3.6 Digital Assets Analytics* for additional information). Also, depending on the digital asset, the data publicly available "on-chain" may differ depending on the design of the underlying blockchain. Per the Office of the Comptroller of the Currency: "Banks should also be aware that different cryptocurrencies may have different technical characteristics and may therefore require risk management procedures specific to that particular currency."[267] As a result of the unique characteristics of digital assets, many standard AML controls and solutions (as currently configured), are not operationally 'native' to virtual currency funds transfers.

Notwithstanding these challenges, FinCEN guidance is clear that any entity, whether DD or money services business, engaging in transactions denominated in value that substitutes for currency, such as digital asset transactions, is subject to BSA regulations, including funds transfer rule or "Travel Rule" requirements.[268] Accordingly, DDs are expected to have policies, procedures, and processes in place to maintain records in a way that permits the reconstruction of individual transactions with transaction details consistent with funds transfer expectations.

---

[266] Consistent with recent proposed rule-making from FinCEN, the Department recognizes the definition of "money" to include convertible funds currencies ("CVC"), including stablecoins.

[267] Office of the Comptroller of the Currency, "Interpretive Letter #1170" (July 2020).

[268] FinCEN Guidance, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," (FIN-2019-G001) (May 2019).

History of Virtual Currency Funds Transfers Regulation

The Bank Secrecy Act ("BSA") was amended by the Annunzio–Wylie Anti-Money Laundering Act of 1992 to authorize the U.S. Treasury and the Federal Reserve Board to prescribe regulations for domestic and international funds transfers.

In 1995, the U.S. Treasury and the Board of Governors of the Federal Reserve System issued a final rule on recordkeeping requirements concerning payment orders by DDs (31 CFR 1020.410)[269]. The rule requires each DD involved in funds transfers[270] to collect and retain certain information in connection with funds transfers of $3,000 or more.[271,272] The information required to be collected and retained depends on the DD's role in the particular funds transfer (originator's DD, intermediary DD, or beneficiary's DD).[273] The requirements may also vary depending on whether an originator or beneficiary is an established customer of a DD and whether a payment order is made in person or otherwise.

Also in 1995, the U.S. Treasury issued a final rule that requires all financial institutions to include certain information in transmittal orders for funds transfers of $3,000 or more (31 CFR 1010.410).[274] This requirement is commonly referred to as the "Travel Rule."

In 2019, FinCEN issued guidance that "transmittal of funds of $3,000 or more (or its equivalent in CVC) may trigger certain requirements on a money transmitter acting as either the financial

---

[269] 31 CFR 1020.410(a) is the recordkeeping rule for DDs, and 31 CFR 1010.410(e) imposes similar requirements for nonbank financial institutions that engage in funds transfers. The procedures in this core overview section address only the rules for banks in 31 CFR 1020.410(a).

[270] Funds transfer is defined under 31 CFR 1010.100. Funds transfers governed by the Electronic Fund Transfer Act of 1978, as well as any other funds transfers that are made through an automated clearing house, an automated teller machine, or a point-of-sale system, are excluded from this definition and exempt from the requirements of 31 CFR 1020.410(a), and 31 CFR 1010.410(e) and (f).

[271] 31 CFR 1020.410(a)(6) provides exceptions to the funds transfer requirements. Funds transfers where both the originator and the beneficiary are the same person and the originator's DD and the beneficiary's DD are the same DD are not subject to the recordkeeping requirements for funds transfers. Additionally, exceptions are provided from the recordkeeping requirements for funds transfers where the originator and beneficiary are: a DD; a wholly owned domestic subsidiary of a DD chartered in the United States; a broker or dealer in securities; a wholly owned domestic subsidiary of a broker or dealer in securities; the United States; a state or local government; or a federal, state or local government agency or instrumentality.

[272] Refer to the DD Custody/Fiduciary Manual ("Valuation of Digital Assets") for additional background on the Department's approach for more information on determining valuation techniques for different digital assets.

[273] These terms are defined under 31 CFR 1010.100.

[274] The rule applies to both banks and nonbanks (31 CFR 1010.410(f)). Because it is broader in scope, the Travel Rule uses more expansive terms, such as "transmittal order" instead of "payment order" and "transmittor's financial institution" instead of "originating bank." The broader terms include the bank-specific terms.

institution for the transmitter or recipient, or as an intermediary financial institution."[275] FinCEN clarified further that: "transactions involving CVC qualify as transmittals of funds, and thus may fall within the Funds Travel Rule."[276] Similarly, in June 2019, the Financial Action Task Force (FATF) updated its guidance to state explicitly that virtual asset service providers, or VASPs,[277] must share accurate sender (originator) and required receiver (beneficiary) information in virtual currency transactions above $1,000. Per the FATF guidance, originating VASPs must transmit mandated data to the beneficiary VASP (if applicable) immediately and securely, ensuring that only those parties processing the transfer have access to the information.[278] However, FATF acknowledged that at the time these recommendations went into effect there did not exist "a technological solution(s) that enabled VASPs to comply with all aspects of the travel rule in a holistic, instantaneous and secure manner."[279] Accordingly, digital asset industry efforts have been underway since 2019 to develop and integrate with solutions that would enable regulated entities to come into compliance with U.S. travel rule requirements and international standards.

Further, in January 2021, FinCEN proposed "establishing new recordkeeping requirements for certain CVC or LTDA transactions that is similar to the recordkeeping and travel rule regulations pertaining to funds transfers and transmittals of funds."[280] The proposed scope of the requirements would include unhosted wallet transactions, which can allow for anonymity and concealment of illicit financial activity. While the proposed FinCEN rule is still pending, trends both within the U.S. and in Europe[281] throughout 2021 and into 2022 are indicative of increased regulatory scrutiny over Travel Rule compliance and pressures on intermediary institutions to put additional recordkeeping and reporting controls around interactions with unhosted wallets. DDs should, therefore, have controls in place to ensure they can adapt to evolving Travel Rule requirements, including proposed rules or guidance that may eventually enter into force around the treatment of unhosted wallets.

---

[275] FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 2019).

[276] Ibid

[277] Per FATF, VASPs are defined as entities that conduct one or more of the following activities: Exchange between virtual assets and fiat currencies; Exchange between one or more forms of virtual assets; Transfer of virtual assets; Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

[278] In more recent guidance from 2021, FATF noted that while "the occasional transaction threshold for CDD is set at USD/EUR 1,000 for virtual asset transfers… a few jurisdictions reported that they had introduced stricter measures than the FATF Standards by introducing a zero-dollar CDD threshold."

[279] FATF, "Second 12 Month Review of Revised FATF Standards - Virtual Assets and VASPs" (July 2021).

[280] FinCEN Proposed Rule, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" (January 2021).

[281] EU Parliament, "EU Parliament Votes to Impose KYC on Private Crypto Wallets" (March 2022).

Industry Challenges Associated with Travel Rule Compliance

Because digital asset transactions are pseudonymous, can be executed swiftly peer-to-peer without regulated intermediaries, and are borderless in nature, Travel Rule compliance has taken significant industry effort.[282] Particular barriers to Travel Rule compliance have included the following:

- Travel Rule information is not required to execute digital asset transactions;
- Regulated entities are generally unable to distinguish between wallet addresses that belong to a regulated intermediary versus an unhosted wallet (and blockchain analytics capabilities are limited in this regard);
- Regulated entities typically do not have the authority and or ability to modify digital asset protocols to capture Travel Rule information in the funds transmission; and
- Effective Travel Rule information transmission requires a single solution or interoperable standards for global information exchange, but adoption occurs at different rates between regulated entities and jurisdictions, and there is no "one solution" in the digital asset space akin to the Society for Worldwide Interbank Financial Telecommunication (SWIFT) standard for execution of financial transactions and payments between banks.

For these reasons, FATF notes in a 2021 annual review on the state of the digital asset industry's compliance with FATF recommendations that: "while there has been progress, there has not yet been sufficient advancement in the global implementation of the travel rule or the development of associated technological solutions." [283] Based on FATF's review, "no jurisdiction advised that they were aware of a VASP which complied fully with each element of the travel rule."[284] Consistent with FATF's observations and given that as of mid-2022 no digital asset service provider is considered fully compliant, digital asset service providers rely on "best efforts" mitigating controls. These mitigating controls may include participation in an industry-led solution that enables trusted members to share information within a permissioned network[285], integration with commercial travel solutions (what FATF refers to as "third party technological solutions for information-sharing"), and manual data collection from customers through deposit and withdrawal questionnaires.

---

[282] FDIC, "Financial Institution Letter: Notification of Engaging in Crypto-Related Activities (FIL-16-2022)" (April 2022).

[283] FATF, "Second 12 Month Review of Revised FATF Standards - Virtual Assets and VASPs" (July 2021).

[284] Ibid

[285] In the U.S., a popular solution that has gained industry traction is Travel Rule Universal Solution Technology ("TRUST"), formerly known as the U.S. Travel Rule Working Group.

Emerging Processes and Technologies around Virtual Currency Compliance for Funds Transfers Recordkeeping

Since the publication of the 2019 FATF guidance, industry working groups and market participants have worked to develop standardized (interoperable) messaging standards as well as messaging software to facilitate compliance with funds transfers record keeping requirements for virtual currencies.

In addition to development of messaging standards, a number of industry stakeholders (including exchanges, technology vendors, and industry working groups) have developed technical solutions to facilitate the exchange of required funds transfer recordkeeping information. ***Note:*** *As an additional control, or interim solution before the integration of a Travel Rule partner/solution, several firms in the digital assets space are utilizing a withdrawal/deposit questionnaire to ensure compliance with the Travel Rule (i.e., capturing the required originator and beneficiary information).*

Regardless of the messaging standards and technical solutions that DDs adopt to meet funds transfer recordkeeping requirements,[286] the Department expects DDs to have policies, processes, procedures, and supporting technology in place to enable and demonstrate compliance for virtual currency funds transfers recordkeeping requirements. This documentation should demonstrate, in a clearly auditable manner, the means through which the DDs send/receive beneficiary or originator information in accordance with funds transfer recordkeeping requirements, and controls in place in the event the DD receives transactions that are non-compliant. Where DDs use multiple off-chain protocols or messaging solutions, DDs should document how and why the solutions are used to meet funds transfer recordkeeping requirements for each virtual currency offered by the DD.

Funds Transfers Transaction Data Requirements

Responsibilities of Originator's DD

Recordkeeping Requirements

For each payment order in the amount of $3,000 or more that a DD accepts as an originator's DD, the DD must obtain and retain the following records (31 CFR 1020.410(a)(1)(i)):

- Name and address of the originator.
- Amount of the payment order.
- Date of the payment order.
- Any payment instructions received from the originator with the payment order.

[286] FATF guidance also sets forth guidance recognizing the need to implement novel solutions to meet funds transfer recordkeeping requirements for virtual currencies.

- Information relating to the originator and beneficiary (including associated virtual currency wallet addresses)[287]
- Transaction details (including virtual currency transaction ID or hash)
- Virtual currency wallet address of the beneficiary
- Identity of the beneficiary's institution.
- As many of the following items as are received with the payment order:
    - Name and address of the beneficiary.
    - Account number of the beneficiary
    - Any other specific identifier of the beneficiary.
- Memo field, if applicable.

Where the DD is the originator institution, the DD should have policies, processes, and procedures in place to record and screen the identity of the beneficiary. Additionally, FinCEN guidance states that the following information is useful to law enforcement and other national security agencies investigating potential illicit conduct involving virtual currency transactions. As part of law enforcement or other requests, DDs may also be asked to retrieve the following information:

- Relevant transaction history
- Available login information (including IP addresses, geolocations, use of VPN)
- Mobile device information (such as device IMEI)
- Information obtained from analysis of the customer's public online profile and communications

Accordingly, DDs should have policies, processes, and procedures in place to demonstrate transaction data collection requirements where the DD is serving as the originating party, with clear data governance processes around how these records are maintained, and integrated into the DD's overall control framework.

Payment Orders Not Made in Person

If a payment order is not made in person, the originator's DD must obtain and retain the following records:

- Name and address of the person placing the payment order.
- The person's TIN (e.g., SSN or EIN) or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof, and a copy or record of the method of payment (e.g., check) for the funds transfer. If the originator's DD has knowledge that the person placing the payment order is not the originator, the

[287] The addition of virtual currency wallet addresses as a required field recognizes the requirement within 31 CFR § 1010.410(f) to include "Any other specific identifier of the beneficiary."

originator's DD must obtain and record the originator's TIN (e.g., SSN or EIN) or, if none, the alien identification number or passport number and country of issuance, or a notation of the lack thereof.

Retrievability

Information retained must be retrievable by reference to the name of the originator. When the originator is an established customer of the DD and has an account used for funds transfers, information retained must also be retrievable by account number (31 CFR 1010.410(a)(4)). Records must be maintained for five years. DDs must have policies, processes, and procedures in place that document operationally how the DD maintain transactions records internally that map to on-chain transaction information to their recordkeeping processes, with adequate oversight to verify there are not gaps in coverage.

Travel Rule Requirement

For funds transmittals of $3,000 or more, the transmitter's financial institution must include the following information in the transmittal order at the time that a transmittal order is sent to a receiving financial institution (31 CFR 1010.410(f)(1)):

- Name of the transmitter, and, if the payment is ordered from an account, the account number of the transmitter (including associated virtual currency wallet addresses).
- Address of the transmitter.
- Amount of the transmittal order.
- Date of the transmittal order.
- Identity of the recipient's financial institution (or virtual currency wallet custodian).
- Account information of the transmitter (including virtual currency wallet addresses associated with the transmitter).
- Transaction details (including virtual currency transaction hash and information on the originator and the recipient).
- Virtual currency wallet address of the recipient.
- As many of the following items as are received with the transmittal order:
    - Name and address of the recipient.
    - Account number of the recipient
    - Any other specific identifier of the recipient.
- Either the name and address or the numerical identifier of the transmitter's financial institution.

***Note**: FinCEN guidance states that the following information is useful to law enforcement and other national security agencies investigating potential illicit conduct involving virtual asset transactions. DDs may be required to retrieve the following information and make it available to law enforcement and other national security agencies:*

- Relevant transaction history
- Available login information (including IP addresses, geolocations, use of VPN)
- Mobile device information (such as device IMEI)
- Information obtained from analysis of the customer's public online profile and communications.

Note: *this section removes the "Responsibilities of Intermediary Institutions" from the FFIEC AML Manual's Funds Transfers Recordkeeping requirements recognizing that all virtual currency funds transfers will be considered direct originator-beneficiary transactions rather than the DD serving in an intermediary capacity.*

Responsibilities of Beneficiary's DDs

Recordkeeping Requirements

For each payment order of $3,000 or more that a DD accepts as a beneficiary's DD, the DD must retain a record of the payment order.

Proceeds Not Delivered in Person

If proceeds are not delivered in person, the institution must retain a copy of the check or other instrument used to effect the payment (including transaction details such as virtual currency transaction hash and information on the originator and the recipient), or the institution must record the information on the instrument. The institution must also record the name, address, and virtual currency wallet address of the person to whom it was sent.

Retrievability

Information retained must be retrievable by reference to the name of the beneficiary. When the beneficiary is an established customer of the institution and has an account used for funds transfers, information retained must also be retrievable by account number (31 CFR 1020.410(a)(4)). DDs must also be able to demonstrate how documented transactions are linked to transactions recorded on the virtual asset's respective blockchain network so that the on-chain transaction information and the off-chain "Travel Rule" information are inextricably linked to facilitate investigations.

There are no Travel Rule requirements for beneficiary DDs.

Abbreviations and Addresses

Although the Travel Rule does not permit the use of coded names or pseudonyms, the rule does allow the use of abbreviated names, names reflecting different accounts of a corporation (e.g., XYZ Payroll Account), and trade and assumed names of a business ("doing business as") or the names of unincorporated divisions or departments of the business.

Customer Address

The term "address," as used in 31 CFR 1010.410(f), is not defined. Previously issued guidance from FinCEN had been interpreted as not allowing the use of mailing addresses in a transmittal order when a street address is known to the transmitter's financial institution. However, in the November 28, 2003, Federal Register notice,[288] FinCEN issued a regulatory interpretation that states the Travel Rule should allow the use of mailing addresses, including post office boxes, in the transmitter address field of transmittal orders in certain circumstances.

The regulatory interpretation states that, for purposes of 31 CFR 1010.410(f), the term "address" means either the transmitter's street address or the transmitter's address maintained in the financial institution's automated CIF (such as a mailing address including a post office box) as long as the institution maintains the transmitter's address[289] on file and the address information is retrievable upon request by law enforcement.

[288] 68 Fed. Reg. 66708 (November 2003).

[289] Consistent with 31 CFR 1020.220, an "address" for purposes of the Travel Rule is as follows: for an individual, "address" is a residential or business street address, an Army Post Office Box or a Fleet Post Office Box, or the residential or business street address of next of kin or another contact person for persons who do not have a residential or business address. For a person other than an individual (such as a corporation, partnership, or trust), "address" is a principal place of business, local office, or other physical location. However, while 31 CFR 1020.220 applies only to new customers opening accounts on or after October 1, 2003, and while the rule exempt funds transfers from the definition of "account," for DDs, the Travel Rule applies to all transmittals of funds of $3,000 or more, whether or not the transmittor is a customer for purposes of 31 CFR 1020.220.

3.7.1. Virtual Currency Funds Transfers Recordkeeping – Examination Procedures

Objective. *Assess the DD's compliance with statutory and regulatory requirements for funds transfers. This section covers the regulatory requirements as set forth in the BSA. Refer to the expanded sections of this manual for discussions and procedures regarding specific money laundering risks for funds transfer activities.*

Note: Department examiners should conduct this review alongside the FFIEC AML Manual's Funds Transfers Recordkeeping section, as warranted based on the DD's risk profile.

Procedure	Comments
1. Verify that the DD obtains and maintains appropriate records for compliance with 31 CFR 1020.410(a).	
2. Verify, as appropriate, that the DD transmits payment information as required by 31 CFR 1010.410(f) (the "Travel Rule") for each virtual currency that the DD supports or facilitates payments. Determine the processes (whether automated or manual) the DD has in place to ensure compliance with the Travel Rule for virtual currency – e.g., integration with an industry travel rule solution, use of a third-party vendor, withdrawal/deposit questionnaire, etc.	
3. Review the DD's policies, processes, and procedures around transaction data collection requirements, including data governance processes around how these records are maintained, and integrated into the DD's overall control framework. Taking a risk-based approach, Department examiners should review these requirements in the context of all virtual currencies supported by the DD.	
4. Review the DD's policies, processes, and procedures around maintaining records for any incoming virtual currency funds transfers that are not in compliance with the	

Procedure	Comments
travel rule, and any additional escalation measures the DD has in place to identify such types of transactions.	
5. Verify that the DD files CTRs when currency is received or disbursed in a funds transfer that exceeds $10,000 (or files VCTRs for its equivalent in CVC, involving both hosted and unhosted wallets, where applicable and required under federal regulation).	
6. If the DD sends or receives funds transfers to or from institutions in other countries, especially those with strict privacy and secrecy laws, assess whether the DD has policies, procedures, and processes to determine whether amounts, the frequency of the transfer, and countries of origin or destination are consistent with the nature of the business or occupation of the customer.	
Transaction Testing	
7. On the basis of a risk assessment, prior examination reports, and a review of the DD's audit findings, select a sample of virtual currency funds transfers processed as an originator's DD and a beneficiary's DD to ensure the institution collects, maintains, or transmits the required information, depending on the institution's role in the transfer. Taking a risk-based approach, conduct a sample for each virtual currency for which the DD offers funds transfers. If the DD offers multiple technology solutions for compliance with funds transfers requirements, select a sample of each method for review.	
8. On the basis of examination procedures completed, review DD records maintained around transactions that were not in compliance with Travel Rule requirements.	

Procedure	Comments
9. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with virtual asset funds transfers.	

3.8. Model Risk Management — Overview

Objective. *Assess the DD's policies, procedures, and processes related to model risk management for models used in AML/CFT and OFAC-related control processes.*

Model risk management (or "MRM") is a critical component of AML/CFT and OFAC oversight. The Department acknowledges DDs may have MRM frameworks that extend beyond AML/CFT and OFAC oversight, although given the likely reliance on models to manage ML/TF and sanctions risks posed by digital assets, MRM is included within this DD AML & OFAC Manual.

The primary supervisory guidance regarding model risk in the United States is the *Supervisory Guidance for Model Risk Management* ("MRM Guidance"), which serves as the main touchstone for regulators' model risk management expectations and regulations.[290] A *model* generates results which are quantitative or categorical estimates, rather than known quantities based on the inputs. Typically, models are processes that use methods based on statistical, economic, financial, or mathematical theory, but they may also be based on expert judgment.

DDs will likely rely on models for a variety of AML/CFT and OFAC controls. AML/CFT and OFAC systems that rely on models frequently include:

- Automated transaction monitoring (both third party and in-house) systems that implement AML/CFT monitoring rules to identify transactions for secondary review and investigations by DD personnel;
- Automated analytics controls involving probabilistic attributions and/or clustering to identify high risk entity exposures;
- Scoring algorithms that rank accounts, customers counterparties (such as virtual asset service providers), and wallet addresses based on ML/TF and sanctions risk;
- Judgmentally developed classification schemes that risk-rank customers for customer risk profiles or CDD purposes;
- Name and address matching algorithms for OFAC sanctions and watch list screening (e.g., PEP and adverse media screening); and
- IP address and geo-location monitoring and blocking, VPN monitoring, and email address monitoring (for prevention of potential OFAC/sanctions violations).

The MRM Guidance sets out supervisors' expectations regarding model governance, development, implementation, validation, and use of both third party and internally-developed models. Consistent with federal supervisory materials, the Department notes that the rigor and sophistication of validation should be commensurate with the DD's overall use of models, the

[290] Federal Reserve Board (SR 11-7) and Office of the Comptroller of the Currency (OCC 2011-12), "Supervisory Guidance on Model Risk Management" (MRM Guidance) (April 2011). (Subsequently issued by the Federal Deposit Insurance Corporation in June 2017 as FIL-22-2017.) Certain regulations, such as those regarding the Swap Margin Rule, have adopted text directly from this guidance.

complexity and materiality of its models, and the size and complexity of the DD's operation, as well as the risk presented by use of individual models within each institution.[291]

Model Governance, Policies, and Controls

Per the MRM Guidance, each model should have an assigned model owner, who is generally the responsible party whom the model is intended to serve. Each model owner is responsible for ensuring the model is appropriately developed or acquired, implemented, used, and subject to proper validation.

An institution's approach to MRM should be set by senior management and formalized through a framework including policies and procedures. Department examiners should assess how the DD emphasizes testing throughout model life as part of model development or change, implementation, validation and on an ongoing basis, and defines acceptable performance standards, where practical. This evaluation may also consider how the framework sets documentation requirements across MRM-related activities, describes model conceptual approach, addresses empirical evidence supporting the methods used and variables selected for the model, documents model limitations and assumptions, and facilitates traceability and auditability of source data used to inform model inputs.[292] Department examiners may also assess how model documentation defines the model's intended use and any proposed restrictions on use as well as documentation around model changes and testing.

Department examiners should assess whether the DD model risk frameworks define the scope and frequency of model validations, with clearly delineated roles and responsibilities. For example, this review could include whether frameworks are subject to annual review by senior management or their delegates. Department examiners should also assess that the model risk framework require an institution to maintain a AML/CFT and OFAC model inventory including models currently in production, under development, or recently retired. An institution's internal audit function or a third party (employed by internal audit with requisite experience) should assess the effectiveness of the model risk management framework design and implementation.

Model Development, Implementation, and Use

Model development is the process by which new models are created or acquired, or model changes are made to existing models. This process is prior to and distinct from model implementation, defined below. The design, theory, and logic of the model should be documented and supported

[291] "The range and rigor of validation activities conducted prior to first use of a model should be in line with the potential risk presented by use of the model." (MRM Guidance, p. 10).

[292] See MRM Guidance, pp. 5-6 and p. 11. For example, in the case of a typical judgmental CRR model, this documentation may include the policies, procedures, and processes associated with collecting the customer input variables, as well as the completeness and quality of these data fields for the relevant population(s). For other models, such as those that require transaction data, this documentation could include screening data completeness and other criteria to verify data lineage and ensure that data feeds flow into the software are understood and functioning as intended.

by published research and industry practice as available. The development effort should include a focus on the quality and relevance of development data,[293] particularly when considering external data. Testing, including output analysis[294] should be an integral part of the development process and should encompass the intended uses for the model.

Implementation describes the preparation of a developed model for regular computer system use and access by the model users. Many model development projects will require the model to be re-coded and/or installed in the production system as part of model implementation. Rewritten code should be tested in parallel with development code and data input and output processes verified. All models will require that applicable security protocols be implemented as part of model implementation. Implementation also includes installing the necessary functionality to support ongoing monitoring, where applicable.

Model use includes the act of running the model to generate output, collating model output to produce reports or populate databases and using that output whether directly from the model, stored in an intermediate database, or in reports to inform business decisions. Model users' understanding of model strengths and weaknesses should be adequate to support effective use and users should report any issues observed to the appropriate parties. Reports produced by users should include information regarding model strengths and weaknesses to inform decision-making.

Model Validation

Department examiners should evaluate the DD's approach to AML/CFT and OFAC model validation, including frequency and performance triggers for review. Consistent with supervisory expectations, models should be subject to validation processes, including initial validation, ongoing monitoring, periodic review, change validation, and periodic re-validation.

- **Initial validation.** The most rigorous validation process, initial validation should be conducted prior to a model's initial use in business processes, and includes review and effective challenge of the model's conceptual soundness, including documentation and evidence supporting both (a) the model's methodology and (b) variables and assumptions selected. The relevance of development data used to build the model, as well as the quality of the model inputs should be included as part of this evaluation.[295] Initial validation may also include sensitivity analysis and outcomes analysis, including back-testing and

[293] Development data includes data used in model selection, design, estimation, testing, and related model development activities.

[294] In the example of a typical judgmental CRR model, output analysis may include sample-based EDD on risk rated customers to assess rating accuracy.

[295] In the example of a typical judgmental customer risk profiling model, testing could include a review of the DD's approach to customer segmentation, review of the justification used for input variables, and evaluation of data completeness and data quality for inputs.

benchmarking, as appropriate.[296] Testing conducted during development which covers these areas may be largely relied upon, subject to effective challenge by the validation staff.

- **Ongoing monitoring.**[297] Ongoing monitoring serves to verify that models are working as intended. The appropriate cycle for ongoing monitoring depends on the nature of the model and its data inputs but should include output analysis, process verification, and review of any model overrides applied to model output. Where applicable, testing should include performance triggers at which the monitoring results will indicate a need for further investigation.[298]
- **Periodic review.**[299] Periodic reviews should be performed to determine whether a model is working as intended and whether existing validation activities are sufficient. Periodic reviews generally assess ongoing monitoring processes and results as well as the quality of data feeding the model; confirm the existing model risk rating is appropriate; assess the adequacy of the current validation activities; review the model change log for non-material changes; and confirm compliance with any restrictions placed on model use.
- **Change validation.**[300] The DD should perform a change validation on any material changes made to the model or its use, prior to deployment of the changed model. A change validation generally involves re-performing relevant elements of the initial validation, although the scope should be determined by the relevant oversight area.
- **Periodic re-validation.**[301] Periodic re-validations are performed on a risk-based frequency as determined by the DD or due to trigger-based events such as changes in regulatory or market conditions, business strategy, or poor performance. Periodic revalidations generally address areas covered in an initial validation for the same model, although the validation team may apply judgment to modify coverage as appropriate.

Models should be validated based on their intended use. Model validation activities should be performed by staff with appropriate incentives, competence, and influence. Except for ongoing monitoring, staff should be independent from the model's development, implementation, or use; capable of understanding and challenging the quantitative concepts applied; and empowered to

---

[296] In the example of a typical judgmental customer risk profiling model, benchmarking may include replicating the CRR model using a different methodology.

[297] "The second core element of the validation process is ongoing monitoring. Such monitoring confirms that the model is appropriately implemented and is being used and is performing as intended. This monitoring should continue periodically over time, with a frequency appropriate to the nature of the model, the availability of new data or modeling approaches, and the magnitude of the risk involved." (MRM Guidance, p. 12).

[298] In the example of a typical judgmental customer risk profiling model, ongoing monitoring may include monitoring the underlying customer base, high-level risk segmentation, and SAR filings.

[299] "Banks should conduct a periodic review—at least annually but more frequently if warranted—of each model to determine whether it is working as intended and if the existing validation activities are sufficient." (MRM Guidance, p. 10).

[300] "Material changes to models should also be subject to validation." Ibid

[301] "It is generally good practice for DDs to ensure that all models undergo the full validation process, as described in the following section, at some fixed interval, including updated documentation of all activities." Ibid

enforce necessary changes. Model validation activities should be documented and archived. When relying on external resources for validation activities, the DD should be responsible for ensuring that a designated internal party can understand and evaluate the results.

Use of Third-Party Models

Vendor models should be incorporated into a DD's broader model risk management framework following the same principles as applied to in-house models, although the process may be somewhat modified. The model owner is responsible for ensuring adequate documentation of vendor models, which generally includes a combination of vendor-supplied and DD-developed reporting. DDs may not be allowed full access to computer code and implementation details for externally developed models, so the DD may have to apply more rigorous testing than for internally developed models. Such testing may include enhanced sensitivity analysis, benchmarking, and other forms of outcomes analysis.

Vendor models are often designed to provide a range of capabilities and so may need to be customized by a DD for its needs. A DD's customization choices should be documented and justified to reflect how the DD has customized the model based on the DD's risk tolerance and profile. The integration of the model into the DD's systems should also be clearly documented (including data lineage/data traceability between DD systems and third-party APIs) through policies, processes, and procedures that explain how the model (e.g., blockchain analytics solution) integrates into the DD's overall control framework consistent with the DD's risk profile.[302] Department examiners should assess the DD vendor selection process (where applicable), including a review of testing procedures used to verify how a third-party or vendor model addresses the DD's intended use for the model.

Department examiners should apply the same expectations to the assessment of vendor model validations and in-house model validations. It is a best practice for vendor model documentation to be subject to effective challenge, including spot-checking of development testing results.[303]

[302] New York Department of Financial Services, "Guidance on Use of Blockchain Analytics" (April 2022).

[303] As part of this review, Department examiners may consider other supervisory guidance around third party risk management, noting that "a financial institution's board of directors and senior management are responsible for identifying and controlling risk arising from third-party relationships to the same extent as if the third-party activity were handled within the institutions." See the FDIC's *Guidance for Managing Third-Party Risk* among other guidance for additional information.

3.8.1. Model Risk Management for DDs — Examination Procedures

Objective. *Assess the DD's policies, procedures, and processes related to MRM for models used in AML/CFT and OFAC-related control processes.*

Procedure	Comments
1. Assess AML/CFT and OFAC MRM model governance to evaluate whether there are clear lines of accountability, including responsible owners for model risk standards and appropriate involvement from senior management.	
2. Assess AML/CFT and OFAC-related models within the DD's model inventory, as well as the DD's model inventory update processes, including frequency of reviews and scope.	
3. Assess the DD's process for model development and implementation for AML/CFT and OFAC models, particularly for appropriate testing and documentation.	
4. On a risk basis, assess the DD's model-specific documentation for AML/CFT and OFAC models, including descriptions of conceptual approach, model use, and data flow for both internally-developed and vendor models.	
5. Review processes to verify AML/CFT and OFAC models are subject to appropriate validation including identification and remediation of issues. Where available, request a copy of the model validation report, including any relevant workpapers, conclusions, and associated remediation efforts.	
6. On a risk basis, review the DD's process to conduct effective challenge for the DDs' AML/CFT and OFAC models.	
7. Review the DD's vendor selection process, including the DD's expertise, to assess its adequacy to meet DD needs.	
8. Assess the DD's customization of vendor models and the associated justifications to	

Procedure	Comments
determine whether DD has customized the model based on its risk profile and risk appetite.	
9. On the basis of examination procedures completed and documentation reviewed, form a conclusion about the adequacy of policies, procedures, and processes associated with AML/CFT and OFAC model risk management.	

3.9. BSA Record Retention Requirements — Overview

Objective. *Assess the DD's policies, procedures, and processes related to recordkeeping and ensure they are in compliance with state and federal requirements.*[304]

This control section is provided as a summary listing, as the Department recognizes the importance of maintaining effective record retention policies, processes, and procedures. Particularly given the evolving nature of digital assets, where a number of recent enforcement actions have noted the failure of financial institutions (or individuals) to maintain appropriate books and records to meet BSA requirements. The Department also recognizes that, because much of the transaction activity around digital assets by definition occurs off-ledger, there may be unique digital-asset-specific considerations that DDs will need to put in place to demonstrate compliance with record retention requirements. Accordingly, DDs should have policies, processes, and procedures in place identifying all types of digital assets subject to record retention requirements, with auditable processes to re-create transaction records.

For comprehensive and current BSA record retention requirements, refer to U.S. Treasury/FinCEN regulations found at 31 CFR Chapter X. These BSA record retention requirements are independent of and in addition to record retention requirements under other laws.

Five-Year Retention for Records as Specified Below

The BSA establishes recordkeeping requirements related to various types of records including: customer accounts (e.g., loan, deposit, trust, or digital asset escrow), BSA filing requirements, and records that document a DD's compliance with the BSA. In general, the BSA requires that a DD maintain most records for at least five years. These records can be maintained in many forms including original, microfilm, electronic, copy, or a reproduction. A DD is not required to keep a separate system of records for each of the BSA requirements; however, a DD must maintain all records in a way that makes them accessible in a reasonable period of time.

The records related to the transactions discussed below must be retained by a DD for five years. However, as noted below, the records related to the identity of a DD customer must be maintained for five years after the account (e.g., loan, deposit, or trust) is closed. Additionally, on a case-by-case basis (e.g., U.S. Treasury Department Order, or law enforcement investigation), a DD may be ordered or requested to maintain some of these records for longer periods.

Extension of Credit in Excess of $10,000 (Not Secured by Real Property)

This record shall contain:

[304] Refer to *3.7. Virtual Currency Funds Transfers Recordkeeping* for additional information specific to "Travel Rule" considerations.

- Name of borrower.
- Address of borrower.
- Amount of credit extended.
- Nature or purpose of loan.
- Date of loan.

International Transactions in Excess of $10,000

A record of any request made, or instructions received or given regarding a transfer of currency or other monetary instruments, checks, funds, investment securities, or credit greater than $10,000 to or from any person, account, or place outside the United States. Such transfers include all cross-border transfers whether denominated in fiat-based currency or digital assets, when the DD reasonably believes the counterparty is physically located overseas.

Signature Cards

A record of each grant of signature authority over each deposit account.

Account Statements

A statement, ledger card, or other record on each deposit account showing each transaction in, or with respect to, that account.

Deposits in Excess of $100

Each deposit slip or credit ticket reflecting a transaction in excess of $100 or the equivalent record for direct deposit or other funds transfer deposit transactions. The slip or ticket must record the amount of any currency involved.

Taxpayer Identification Number

A record of the TIN of any customer opening an account. In cases of joint accounts, information on a person with a financial interest must be maintained. (If the person is a nonresident alien (NRA), record the passport number or a description of some other government document used to verify identity.) This information must be recorded within 30 days of the date the transaction occurs. In the event a DD is unable to secure the information, it must maintain a list containing the names, addresses, and account numbers of those members for whom it has been unable to secure the information.

Exceptions. A DD does not need to maintain TIN for accounts or transactions with the following:

- Agencies and instrumentalities of federal, state, local, or foreign governments.
- Judges, public officials, or clerks of courts of record as custodians of funds in controversy or under the control of the court.
- Certain aliens as specified in 31 CFR 1020.410(b)(3)(iii-vi).

- Certain tax exempt organizations and units of tax-exempt organizations 31 CFR 1020.410(b)(3)(vii)).
- A person under 18 years of age with respect to an account opened as a part of a school thrift savings program, provided the annual dividend is less than $10.
- A person opening a Christmas club, vacation club, and similar installment savings programs, provided the annual dividend is less than $10.
- NRAs who are not engaged in a trade or business in the United States.

Suspicious Activity Report and Supporting Documentation

A DD must maintain a record of any SAR filed and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing.

Currency Transaction Report

A DD must maintain a record of all CTR for a period of five years from the date of filing.

Designation of Exempt Person

A DD must maintain a record of all designation of persons exempt from CTR reporting as filed with the Treasury for a period of five years from the designation date.

Customer Identification Program

A DD must maintain a record of all information it obtains under its procedures for implementing its CIP. At a minimum, these records must include the following:

- All identifying information about a customer (e.g., name, date of birth, address, and TIN).
- A description of the document that the DD relied upon to identity of the customer.
- A description of the nondocumentary methods and results of any measures the DD took to verify the identity of the customer.
- A description of the DD's resolution of any substantive discrepancy discovered when verifying the identifying information obtained.

A DD must retain the identifying information about a customer for a period of five years after the date the account is closed.

A DD must retain the information relied on, methods used to verify identity, and resolution of discrepancies for a period of five years after the record is made.

As noted, these BSA recordkeeping requirements are independent of and in addition to requirements to file and retain reports imposed by other laws. For the meaning of the BSA terms, see 31 CFR 1010.100.

Comprehensive Iran Sanctions, Accountability and Divestment Act

A DD must retain a copy of any report filed with FinCEN and any supporting documentation, including the foreign DD certification or other responses to an inquiry, for a period of five years (31 CFR 1060.300).

In addition to the above recordkeeping requirements, DDs are required to maintain appropriate records in compliance with 31 CFR 1020.410(a). Refer to *Section 3.7.* on Virtual Currency Funds Transfers Recordkeeping.

3.9.1. BSA Record Retention Requirements — Examination Procedures

Objective. *Assess the DD's policies, procedures, and processes related to recordkeeping and ensure they are in compliance with state and federal requirements.*

Procedure	Comments
1. Review the DD's policies, processes, and procedures around record retention requirements, including: • Extensions of Credit in Excess of $10,000 (Not Secured by Real Property) • International Transactions in Excess of $10,000 • Signature Cards • Account Statements • Deposits in Excess of $100 • Suspicious Activity Report and Supporting Documentation • Currency Transaction Report • Designation of Exempt Person • Customer Identification Program • Comprehensive Iran Sanctions, Accountability and Divestment Act In addition to the above recordkeeping requirements, confirm that the DD maintains appropriate records in compliance with 31 CFR 1020.410(a) pertaining to Virtual Currency Funds Transfers.	
2. Review the DD's record retention schedule.	
3. On the basis of examination procedures completed, including transaction testing and, as applicable, findings from the review of the DD's virtual currency funds transfers, form a conclusion about the ability of policies, procedures, and processes to meet record retention requirements.	

4. DD RISKS ASSOCIATED WITH MONEY LAUNDERING AND TERRORIST FINANCING

4.1. On-off Ramp Exchange and Virtual Currency Funds Transfers — Overview

Objective. *Assess the adequacy of the DD's systems to manage the risks associated with on-off ramp exchange and virtual currency funds transfer, and management's ability to implement effective monitoring and reporting systems. This section expands the core review of the statutory and regulatory requirements of funds transfers to provide a broader assessment of AML risks associated with this activity.*

Virtual Currency Funds Transfers

The underlying technologies (i.e., blockchain) of virtual currencies[305] enables the near-instantaneous transfer of funds that can be executed absent a third-party intermediary, often without involving a regulated financial institution as part of the transfer.

As previously noted, the ability of owners of virtual currencies to transfer ownership without the use of a regulated third party (e.g., between unhosted wallets or to or from an un-registered foreign MSB), creates novel issues to implementing an effective AML/CFT and OFAC compliance program. Information stored on the blockchain ledger (or "on-chain") contains certain identifying information, including sender/receiver wallet addresses, time and date, and value of the transaction. However, this information is generally pseudonymous, with nothing on the face of the transfer tying back to the originator, beneficiary, or underlying beneficial owners. Per the OCC: "…different cryptocurrencies may have different technical characteristics and may therefore require risk management procedures specific to that particular currency."[306]

Additionally, new types of anonymity-enhanced digital assets have emerged that further reduce transparency of transactions and identities involved, but have legitimate uses when accompanied by appropriate controls. These types of digital assets obscure the source of the transaction through the incorporation of anonymizing features, such as mixing and cryptographic enhancements, further increasing the difficulty of DDs' efforts to combat money laundering, terrorist financing, and other financial crimes facilitated through virtual currencies.

DD customers may conduct virtual currency transfers through four methods:

---

[305] Per the Department's approach, the Department recognizes the definition of "money" to include CVCs, including stablecoins.

[306] OCC, "Interpretive Letter #1170" (July 2020).

- Virtual currency on-ramps.
- Virtual currency exchange.
- Virtual currency off-ramps.
- External virtual currency transfers into or out of a DD.

Virtual Currency On-Ramps

A virtual currency on-ramp describes how a DD customer converts fiat currency to a virtual currency. In this scenario, the DD allows for customers to have on-balance sheet, USD-denominated or other fiat-based deposits with a process for customers to convert fiat-based currency into ownership of a digital asset.

Virtual Currency Exchange

A virtual currency exchange typically includes the transfer of one virtual currency into another virtual currency, using a virtual currency as a means of payment.

Virtual Currency Off-Ramps

A virtual currency off-ramp typically describes where a DD customer converts a virtual currency back into fiat currency (i.e., "cashing out"), using a virtual currency as a means of payment. These ramps can be described as the "gateways to and from (i.e., the on and off ramps to) the traditional regulated financial system, in particular convertible virtual currency exchangers."[307]

External Virtual Currency Transfers into or out of a DD

An external virtual currency transfer occurs when a DD customer transfers a digital asset to or from an unhosted wallet, third-party VASP, DD, or other means, into or out of a DD.

Risk Factors

Virtual currency funds transfers present a heightened risk depending on whether the activity is occurring between a DD's customers within the DD's systems or whether there is inbound or outbound activity exogenous to the DD's internal systems (e.g., through an external virtual currency to or from a DD customer's unhosted wallet) as well as based on the nature of the virtual

[307] FATF, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (June 2019).

currency itself. For example, the ability of users to, "make or accept payments in money from/to unknown or un-associated third parties,"[308] is a risk factor for virtual currency funds transfers.

These challenges are exacerbated by the lack of a uniform messaging standard among virtual asset service providers, where, absent mitigating controls the DD's transaction activity could expose the DD to counterparties in jurisdictions that do not have adequate AML/CFT and OFAC controls. Lack of messaging standards for the sending or receiving of information that is not included "on-chain" introduces additional risk as DDs need to incorporate "off-chain" solutions to have adequate transaction details around such virtual currency funds transfers. Without this data, the DD is unable to monitor or filter (i.e., conduct sanctions screening) of payment information, and may face additional challenges around meeting recordkeeping requirements.

Certain virtual currency funds transfers are especially high-risk where a significant proportion of the virtual assets are, "held or used in a transaction that is associated with privacy-enhancing features or products and services that potentially obfuscate transactions or undermine a firm's ability to know its customers and implement effective AML/CTF controls, such as:

- Mixers or tumblers, in the absence of a legitimate privacy or IT security concern;
- Obfuscated ledger technology;
- Internet Protocol (IP) anonymizers;
- Ring signatures;[309]
- Stealth addresses;[310]
- Ring confidential transactions;[311]
- Atomic swaps;[312]
- Non-interactive zero-knowledge proofs;[313]
- Privacy coins without a legitimate use; and

---

[308] UK Joint Money Laundering Steering Committee Group, "*Cryptoasset exchange providers and custodian wallet providers"* (July 2020).

[309] A ring signature is a type of digital signature that can be produced by multiple different users without revealing which member actually produced the signature. Ring signatures as technique can be used to anonymize sender information for certain types of digital assets transaction activity on the public blockchain.

[310] A stealth address is a type of privacy-enhancing approach to digital asset addresses that typically uses a combination of public and private keys to enhance the recipient's privacy on the public blockchain.

[311] A variation of a ring signature which results in a digital currency with hidden amounts, origins and destinations of transactions.

[312] An atomic swap is a type of smart contract technology that enables the peer-to-peer exchange of digital assets from one party to another absent the use of a centralized intermediary, such as an exchange.

[313] A zero-knowledge proof or zero-knowledge protocol is a method by which one party can prove to another party that they know a value x, without conveying any information apart from the fact that they know the value. Non-interactive zero-knowledge proofs typically refer to zero-knowledge proofs that do not require interactions between the prover and the verifier and are a type of cryptographic technique employed in AEC transactions.

- A significant proportion of the [assets are] held or used in a transaction is associated with second-party escrow services."[314]

The use of off-chain digital asset channels such as the Lightning Network Protocol, which facilitate rapid transactions and exchanges of digital assets outside of the native assets blockchain protocol (i.e., without posting to the ledger) may present higher risks for compliance with existing standards absent mitigating controls (e.g., around recordkeeping).

Historical Associations with Illicit Activity

Blockchain's ability to remove a moderating third-party, along with the pseudonymity it can provide, has made virtual currencies a target for criminal activity. This activity has included the use of virtual currencies in ransomware and online scams, as well as on darknet marketplaces to facilitate illicit activity, including fentanyl and heroin trafficking.[315] An updated advisory from FinCEN published in November 2021 identified "new trends and typologies of ransomware and associated payments, including the growing proliferation of AECs and decentralized mixers."[316] Such activity often involves peer to peer (P2P) or unregulated exchanges that allow individuals to transact in virtual currencies without appropriate KYC or CDD. Virtual currency on-ramps and off-ramps are a critical step towards preventing the introduction of illicit funds into the banking system. Some of the key risk factors that DDs should review include substantial exposure to:

- Darknet marketplaces;
- High-risk or sanctioned jurisdictions;
- Wallets from known scams, fraud schemes or ransomware wallets;
- P2P exchanges;
- Unregistered and foreign-located MSBs;
- CVC kiosks;
- Attempted concealment of identity and source of funds;
- Privacy coins used by customers without a legitimate use and other AECs or anonymity-enhancing technology;
- Online gambling and gaming;
- Decentralized mixers; and
- Decentralized exchanges.

---

[314] UK Joint Money Laundering Steering Committee Group, "*Cryptoasset exchange providers and custodian wallet providers"* (July 2020).

[315] FinCEN, "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 2019).

[316] FinCEN, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" (November 2021).

Refer to *Appendix B. Money Laundering and Terrorist Financing Red Flags Associated with Digital Assets* for a more complete discussion of risk associated with virtual currencies.

Varying AML Standards among Virtual Asset Service Providers

Frameworks across VASPs vary significantly with respect to the adoption of compliance standards consistent with AML/CFT and OFAC requirements. Accordingly, DDs should have policies, processes, and procedures to identify how they can obtain and/or screen incoming or outgoing message details around third-party originating or beneficiary institutions.

A DD should consider the countries or jurisdictions it is directly or indirectly exposed to through its activity and the activity of its customers, particularly those countries and jurisdictions "with relatively higher levels of corruption, organised crime or inadequate AML/CFT measures, as identified by the Financial Action Task Force ("FATF")." [317]

Varying Message Protocol Standards

Although there have been recent developments within the industry, exchanges and other operators within the digital assets space do not yet have a coordinated messaging protocol to screen transaction details "off-chain" or to otherwise supplement data available on the blockchain. "There are various technologies and tools available that could enable VASPs to comply with aspects of the travel rule requirements."[318] A number of technology solutions providers and industry working groups have developed offerings including global VASP registries, interoperable messaging protocols, and vendor solutions to address the incomplete information provided as part of completing a transaction on most blockchains.[319] However, a number of these solutions remain either limited in application (e.g., with only a select number of participants) or still in proof-of-concept development stages. In 2021, FATF acknowledged the lack of advancement in the implementation of travel rule solutions globally. FATF encouraged its members to implement

[317] Monetary Authority of Singapore, "Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism" (March 2020).

[318] FATF, "12-Month Review Of The Revised FATF Standards On Virtual Assets And Virtual Asset Service Providers" (June 2020).

[319] In its 2019 guidance, FATF notes different mechanisms to address requirements could include "a solution for obtaining, holding, and transmitting the required information (in addition to complying with the various other requirements of Recommendation 16) could be code that is built into the virtual asset transfer's underlying DLT transaction protocol or that runs on top of the DLT platform (e.g., using a smart contract, multiple-signature, or any other technology); an independent (i.e., non-DLT) messaging platform or application program interface (API); or any other effective means for complying."

travel rule into their domestic legislation and collaborate with the private sector and other countries to facilitate the collection of originator/beneficiary information.[320]

Risk Mitigation

Virtual currency funds transfers can be used in the placement, layering, and integration stages of money laundering. Fiat deposits through virtual currency kiosks are a prototypical example of the placement stage. Detecting unusual activity in the layering and integration stages is more difficult for a DD because transactions may appear legitimate or may otherwise be associated with multiple transfers that challenge a DD's ability to identify an illicit origin of funds. In many cases, a DD may not be involved in the placement of the funds or in the final integration, and may serve as an unwitting intermediary in the layering of transactions. DDs should consider all three stages of money laundering when evaluating or assessing funds transfer risks and should establish sound policies, procedures, and processes to manage the AML/CFT risks of virtual currency funds transfer activities. Such policies may encompass more than regulatory recordkeeping minimums and be expanded to cover OFAC obligations.

Obtaining accurate CDD information and counterparty message details is a requirement for the sending and receipt of funds transfers, including for funds transfers involving virtual currencies. As identified above, the nature of virtual currencies requires unique solutions to identify counterparty information to meet AML/CFT and OFAC requirements. Accordingly, for each type of transaction (including virtual currency on-ramps, virtual currency off-ramps, and external virtual currency transfers) DDs should have policies, procedures, and processes to measure how they are able to address relevant requirements. For example, DDs should define what technology solutions help bridge the lack of verified transaction information present on the blockchain for external virtual currency transactions. DDs should also have policies, procedures, and processes to identify the specific risk criteria associated with ***each virtual currency*** supported by the DD, as well as risk mitigation strategies to address these virtual currency-specific risks. For example, DDs should have processes to identify what **types** of higher-risk digital assets transfers (e.g., privacy coins) may trigger enhanced due diligence requirements including trigger-based customer reviews and/or restrictions such as limits on transaction volume and value, consistent with a customer's intended purpose of the account.

To address these risks, the Department sets forth a risk-based approach for DDs including screening ownership of counterparty wallet addresses as reasonably practicable on a risk basis, with auditable processes. Refer to the table below for illustrative risk measures based on different types of virtual currency transfers.

[320] FATF, "Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers" (July 2021).

Illustrative Scenarios for Virtual Currency Funds Transfers[321]

Origin/Source	Verification Methods
To/from DD account (DD custodial wallet) to/from DD customer's own unhosted wallet	• Screening of ownership of wallet address by customer, as reasonably practicable under the circumstances on a risk-focused basis with auditable processes to recreate screening. • Review against intended purpose of business accounts as appropriate.
To/from DD account (DD custodial wallet) to/from non-DD customer with an account (custodial wallet) at a U.S. regulated bank, U.S. trust company, U.S.-licensed money transmitter[322] or other U.S.-supervised exchange	• Risk-based due diligence on counterparty, which may include documentation of beneficial ownership and screening against lists for sanctions prior to processing of payment. • May include independent verification (e.g., via analytics software) with ongoing monitoring of wallet address. • Review against intended purpose of business accounts. • Confirmation of ability to meet funds transfers requirements.
To/from DD account (DD custodial wallet) to/from non-DD customer with an account (custodial wallet) at a financial institution located in a trusted regulated jurisdiction [323]	• Risk-based due diligence on counterparty, which may include documentation of beneficial ownership and screening against lists for sanctions prior to processing of payment. • May include independent verification (e.g., via analytics software) with ongoing monitoring of wallet address. • Review against intended purpose of business accounts. • Confirmation of ability to meet funds transfer requirements.
To/from DD account to/from non-customer's unhosted wallet	• Risk-based enhanced due diligence on counterparty, including pre-authorization with enhanced due diligence for non-customer addresses and other appropriate risk management processes. • Alternatively, the DD may apply a risk-based decision to make these types of transactions impermissible.

[321] In all such instances, the DD may require additional information from the customer, such as through a deposit or withdrawal questionnaire, to identify the counterparty to the transaction where the counterparty wallet address is unlabeled (within the DD's blockchain analytics tool(s)) and/or where the DD lacks the capabilities to perform

Additionally, a number of blockchain analytics software providers have built solutions to identify (and create risk profiles or risk scores of) owners of wallet addresses, especially VASPs and other institutions. DDs should have processes to demonstrate how they are able to leverage such vendor solutions (or in-house capabilities) to identify and, at minimum, perform real time or pre-transaction screening on the counterparty's wallet address ***prior to processing*** an outbound (off-platform) virtual currency funds transfer. Refer to the *3.6. Digital Asset Analytics* control section for an overview of digital asset analytics service offerings available to address certain risks associated with virtual currency funds transfers.

In addition, an effective risk-based suspicious activity monitoring and reporting system is equally important. Whether this monitoring and reporting system is automated or manual, it should be sufficient to detect suspicious trends and patterns typically associated with money laundering for activity that passes through the DD. Effective monitoring includes:

- Monitoring funds transfers processed through automated systems in order to identify suspicious activity. This monitoring may be conducted after the transfers are processed, on an automated basis, and may use a risk-based approach. In conjunction with open permissioned blockchain data, blockchain analytics software can provide DDs with useful transaction message details for monitoring of digital asset funds transfers (e.g., to map on-chain data for ingestion into traditional transaction monitoring systems or build within the tool).
- Given the volume of messages and data for many U.S. DDs, a manual review of every digital funds transfer may not be feasible or effective. However, DDs should have, as part of their monitoring processes, a risk-based method to identify suspicious transaction activity.

Refer to *3.3. Suspicious Activity Reporting* for considerations around transaction monitoring considerations for virtual currencies.

---

information exchange with the counterparty (e.g., in the case of another VASP where a travel rule process has not been stood up).

[322] E.g., a trust company or money transmitter supervised by another U.S. financial regulator/supervisor which, in the opinion of the Department, appropriately supervises the counterparty financial institution on a regular basis. The U.S. supervisor should also have AML/CFT and sanctions regulations specific to digital assets. Whether or not the jurisdiction has an information-sharing agreement with the Department or federal agencies may also be a factor.

[323] E.g., a jurisdiction which, in the opinion of the Department, has substantially similar AML/CFT and sanctions regulations to the United States and has licensed and appropriately supervises the counterparty financial institution on a regular basis, commensurate with these regulations. The jurisdiction should also have AML/CFT and sanctions regulations specific to digital assets and should not be a jurisdiction cited or known for AML or sanctions deficiencies. Whether or not the jurisdiction has an information-sharing agreement with the Department or federal agencies may also be a factor.

In addition to standard recordkeeping requirements, as part of recent guidance, FinCEN has provided specific areas around customer and transaction information requirements, such as virtual currency wallet addresses, transaction details (including virtual currency transaction hash and information on the originator and the recipient), and available login information (including IP addresses, geolocation, use of VPN). For a more detailed discussion on considerations around transactions-related record retention, refer to *3.7. Virtual Currency Funds Transfers Recordkeeping* and *3.9. BSA Record Retention Requirements*.

4.1.1. On-off Ramp Exchange and Virtual Currency Fund Transfers — Examination Procedures

Objective. *Assess the adequacy of the DD's systems to manage the risks associated with funds transfers, and management's ability to implement effective monitoring and reporting systems. This section expands the core review of the statutory and regulatory requirements of funds transfers to provide a broader assessment of AML risks associated with this activity.*

Procedure	Comments
1. Review the policies, procedures, and processes related to virtual currency funds transfers. Evaluate the adequacy of the policies, procedures, and processes given the DD's virtual currency funds transfer activities and the risks they present. Assess whether the controls are adequate to reasonably protect the DD from money laundering and terrorist financing, as well as OFAC considerations.	
2. Review MIS and internal risk rating factors, and determine whether the DD effectively identifies and monitors virtual currency funds transfer activities.	
3. For each type of virtual currency transaction (including virtual currency on-ramps, virtual currency off-ramps, and external virtual currency transfers *for* ***each virtual currency*** that the DD offers, on a sample basis), evaluate the processes in place to screen customer information for each originator and beneficiary on a sample-basis.	
4. Determine whether an audit trail of virtual currency funds transfer activities exists. Determine whether an adequate separation of duties or other compensating controls are in place to ensure proper authorization for sending and receiving virtual currency funds transfers and for correcting postings to accounts.	
5. Determine whether the DD's system for monitoring virtual currency funds transfers and for reporting suspicious activities is adequate given the DD's size, complexity,	

Procedure	Comments

location, and types of customer relationships. For each virtual currency transaction type that the DD offers, determine whether suspicious activity monitoring and reporting systems include:
• Virtual currency funds transfers purchased with currency.
• Virtual currency to virtual currency funds transfers
  o External virtual currency transfers to or from unhosted wallets
  o Virtual currency transfers from internal custodial wallets to external custodial wallets
• Fiat to virtual currency funds transfers
• Virtual currency to fiat funds transfers
• Transactions in which the DD is originating or receiving virtual currency funds transfers from foreign financial institutions, particularly to or from jurisdictions with strict privacy and secrecy laws or those identified as higher risk.
• Frequent virtual currency deposits or funds transfers and then subsequent transfers, particularly to a larger institution or out of the country.	

6. Review the DD's procedures for virtual currency funds transfers: • Determine whether the DD's processes for risk profiling of wallet addresses and counterparty institutions (e.g., VASPs) reflects an auditable approach to screen counterparty information, as reasonably practicable and in accordance with industry standard. • Determine whether the DD's processes for VASP counter-party due diligence includes the review and the evaluation of the VASP's AML/CFT controls and "Travel Rule" compliance, as reasonably	

Procedure	Comments
practicable and in accordance with industry standard. • Assess the DD's policies for cooperating with its counterparties when they request the DD to provide information about parties involved in virtual currency funds transfers. • Assess the adequacy of the DD's procedures for addressing isolated as well as, repeated instances where virtual currency payment information received from a counterparty is missing, manifestly meaningless or incomplete, or suspicious, and what internal processes are in place to resolve such deficiencies.	
7. Review what procedures the DD has in place to conduct transaction screening of counterparties for each external virtual currency transfer that the DD offers. Refer to *2.4. Assessing the OFAC Compliance Program* for more information.	
Transaction Testing	
8. On the basis of the DD's risk assessment of virtual currency funds transfer activities, as well as prior examination and audit reports, select a sample of virtual currency funds transfer activities for each virtual currency for which the DD offers, which may include the following: • Fiat to virtual currency funds transfers • Virtual currency to fiat funds transfers Virtual currency to virtual currency funds transfers within the DD • External virtual currency transfers to or from unhosted customer wallets • Virtual currency transfers from internal custodial wallets to external custodial wallets	
9. From the sample selected, analyze virtual currency funds transfers to determine whether	

Procedure	Comments
the amount, frequency, and jurisdictions of origin or destination are consistent with the nature of the business or occupation of the customer.	
10. Regardless of the format that DD uses (e.g., via an independent messaging platform), review a sample of messages to determine whether the DD has used the appropriate message formats and has included complete originator and beneficiary information (e.g., no missing or meaningless information).	
11. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with virtual currency funds transfer activity.	

4.2. Staking-as-a-Service for DDs — Overview

Objective. *Assess the adequacy of the DD's policies, procedures, and processes to manage the risks associated with staking-as-a-service, and management's ability to implement effective due diligence, monitoring, and reporting systems.*

Note: Department examiners should review the DD's staking-as-a-service activities in addition to standard FFIEC AML Manual's Concentration Accounts control processes as warranted to form an overall view.

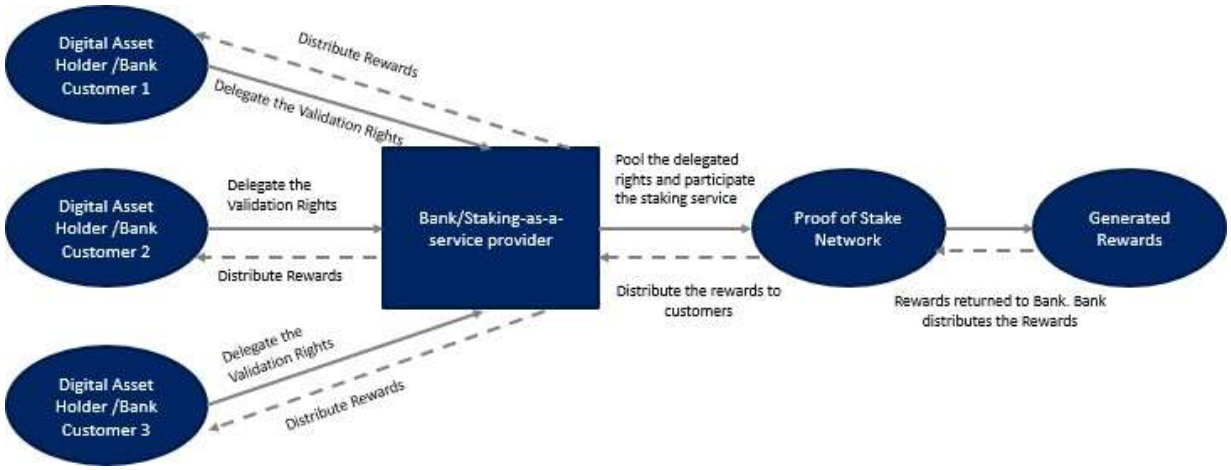
Many digital assets utilize a blockchain network with a "proof-of-stake" consensus mechanism to validate transactions. In a "proof-of-stake" blockchain, network participants (or "nodes") can lock (or "stake") the network's native asset in a digital asset wallet in order to be eligible to validate the next block and earn rewards. "Proof-of-stake" consensus mechanisms, as contrasted with "proof-of-work" consensus mechanisms, do not involve a "competition" between all miners on the network; rather, "proof-of-stake" algorithms use a pseudo-random election process to select a network participant to be the validator of the next block, based on a combination of factors depending on the blockchain network, which could include the staking age (i.e., the length of time the node has been staking on the network), randomization, and the node's digital assets under possession (i.e., quantum of the native asset staked). In exchange for helping to support the security and operations of the blockchain, network participants who stake their virtual assets receive a block reward. A block reward can be (depending on the underlying blockchain) a newly minted virtual asset or a transaction fee from the block that was added (or "forged"). In order to deter malicious behavior, validator nodes that do not adhere to the established rules for validating transaction may face penalties including the forfeiture of funds (these penalties are typically referred to as "slashing").

To earn rewards through staking, network participants must transfer their digital assets to a suitable wallet (or "stake" their virtual assets); staked digital assets typically cannot be spent while they are staked on the network (i.e., "lock up" period). Staking rewards are attributed to "stakers" using a combination of random selection and the size of the stake, often measured by the number of staked digital assets. Typically, the larger the stake, the more likely the "staker" will be selected to validate the next block and receive the block reward. Certain blockchain networks determine the amount of the reward as a fixed percentage while other networks take factors such as the node's wealth, staking age, total network size, and the digital asset inflation rate into consideration. In certain blockchain networks, "stakers" are required to hold their staked digital assets in a suitable digital asset wallet for a pre-determined length of time in order to be eligible to earn rewards.

Digital asset requirements (such as minimum digital asset thresholds required for staking) and the technical complexity of staking, often makes staking infeasible for individual investors. DDs may provide staking services to their customers as a way for the customers to generate passive income (sometimes referred to as "yield") on their digital assets similar to earning interest in a traditional savings account. Staking services pool staked virtual assets from many investors (ensuring digital asset threshold requirements are met) as well as handle the technical aspects of staking, thus

removing many of the barriers to "staking" for investors. Depending on the underlying blockchain's design, staking pools may require the aggregation of staked assets into a single shared digital asset wallet controlled by the staking service provider. Other blockchain designs (such as delegated-proof-of-stake designs) permit the delegation of staked assets, allowing staking pools to operate without the need for the staking service provider to assume custody over the staked digital assets in a single digital asset wallet. Staking services typically charge a fee as a proportion of the rewards. Rewards earned through staking service providers are re-distributed to investors with the staking service provider usually taking a percentage of the attributed block rewards as a fee.

"Staking-as-a-Service" Illustrative Example[324]*:*



Risk Factors:

Due to the nature of "staking-as-service", digital assets from many investors are often pooled into a single omnibus account ("staking pool") to optimize the block reward yield. Moreover, staking-as-service providers can provide their offering as a standalone service, and the "staking pools" created by staking-as-a-service providers can potentially be viewed by illicit actors as an opportunity to launder illicit funds (e.g., digital assets procured through ransomware) through obfuscation of the source of funds.

Absent mitigating controls on the part of a staking-as-a service provider, an illicit actor could deposit tainted digital assets derived from illegal activity into a digital asset wallet to be used for "staking." These tainted digital assets would be pooled/comingled with other investors' digital assets in a "staking pool." The illicit actor would subsequently earn "interest" or "yield" from the tainted assets. The subsequent yield earned through "staking" on these assets would not be

[324] Note this example is illustrative. Where DDs offer staking-as-a-service, Department examiners should assess for adequacy of workflows and DD documentation for that digital asset's staking-as-a-service protocols, and identify whether transaction testing is warranted.

considered tainted and could then be freely "off-ramped" for fiat, other products and services, or exchanged for other digital assets.

Further, when the illicit actor ultimately withdraws their staked assets from the omnibus account, the original source of funds may become more difficult to trace, particularly where the assets have been comingled with other legitimate digital assets (akin to a tumbler/ mixer), effectively resulting in both interest on the original tainted assets, and laundering of the tainted digital assets to appear clean as a result of comingling in the omnibus account.

Risk Mitigation:

Where a DD interacts with an exogenous staking-as-a-service provider, the DD should be attendant to the unique risks associated with "staking pools," as well as the use of omnibus accounts, just as it would be when interacting with digital asset exchanges, and similarly seek to determine what controls the staking-as-a-service provider maintains to mitigate against the risks of high-risk deposits, including whether the staking-as-a-service provider performs KYC and provenance analysis/funds tracing on deposited digital assets.

As part of its due diligence, DDs should have policies, processes, and procedures to screen the source of wealth/funds for customers participating in "staking," for customers that claim their source of funds as originating from external staking pools, and for customers that come to the DD to request staking-as-service in the absence of other product offerings. Additionally, DDs should have appropriate transaction monitoring to identify unusual activity associated with deposits from "staking pools."

The risks of "staking pools" summarized above are primarily associated with the DD's exposure to external staking-as-a-service providers or where the DD offers staking-as-a-service as a standalone product offering in the absence of digital asset custody. Where the DD is providing its own staking-as-a-service offering as a subsequent, or auxiliary service, for digital assets already held in custody for existing customers, the provision of staking services would generally not be considered to result in an elevated risk due to the following two reasons: 1) the funds are endogenous to the DDs internal ecosystem and have already presumably been subject to provenance analysis on the incoming deposit and the customer has been subject to KYC; and 2) the assets are staked by the DD on behalf of the customer but the customer cannot independently control the movement of funds and cannot transfer the funds to a third party. Moreover, due to the nature of staking, which is generally associated with extended funds "lock-up" periods, the service may ultimately be perceived as a less attractive vehicle for money laundering given that the value of the "locked up" digital asset may depreciate over time and cannot be easily moved.

4.2.1. Staking-as-a-Service for DDs — Examination Procedures

Objective. *Assess the adequacy of the DD's policies, procedures, and processes to manage the risks associated with staking-as-a-service, and management's ability to implement effective due diligence, monitoring, and reporting systems.*

Procedure	Comments
1. Review the policies, procedures, and processes related to the DD's staking-as-a-service operations and exposures to external staking-as-a-service operations. Evaluate the adequacy of the policies, procedures, and processes given the DD's activities and the risks they present. Assess whether the controls are adequate to reasonably protect the DD from money laundering and terrorist financing.	
2. Review the DD's procedures for gathering additional identification information, when necessary, about staking-as-a-service customers and customers that deposit funds from external staking-as-a-service providers.	
3. Review the DD's procedures regarding access criteria (e.g., customer onboarding prior to accepting deposits for/from staking).	
4. Determine whether the DD's system for monitoring staking-as-a-service customer relationships for suspicious activities, and for reporting of suspicious activities, is adequate given the DD's size, complexity, location, and types of customer relationships.	
5. If appropriate, for additional guidance refer to the core examination procedures contained in *2.4. Assessing the OFAC Compliance Program*.	
Transaction Testing	

Procedure	Comments
6. On the basis of the DD's risk assessment of its trust and asset management relationships, as well as prior examination and audit reports, select a sample of higher-risk customer relationships. From the sample selected, perform the following examination procedures: • Review account opening documentation, including the CIP, to ensure that adequate due diligence has been performed and that appropriate records are maintained. • Review account statements and, as necessary, specific transaction details. Compare expected transactions with actual activity. • Determine whether actual activity is consistent with the nature of the customer's business and the stated purpose of the account. • Identify any unusual or suspicious activity.	
7. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with staking-as-a-service customer relationships and exposures to external staking-as-a-service providers and deposits.	

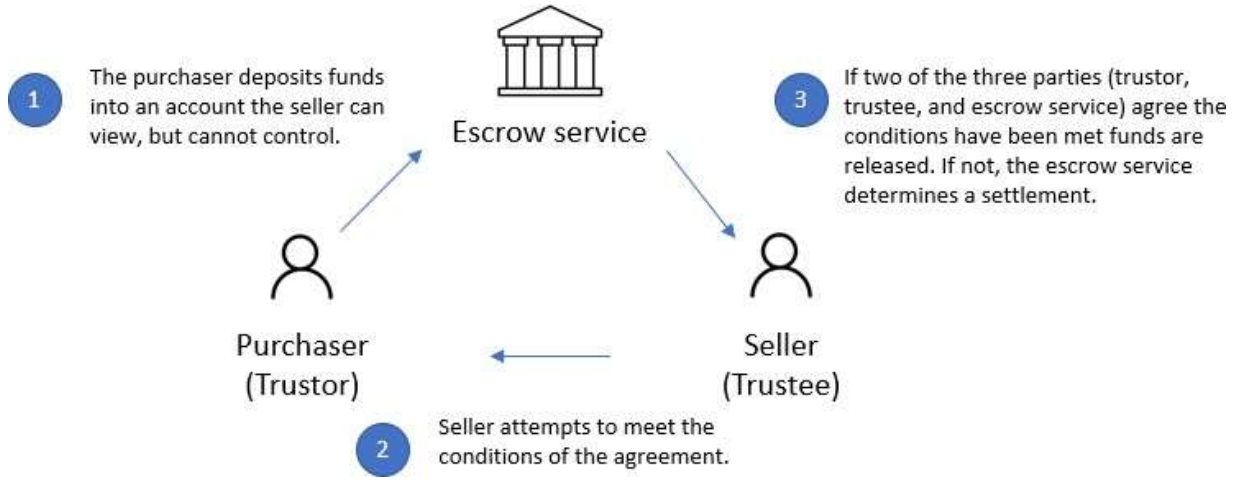
4.3. Digital Assets Escrow Services — Overview

Objective. *Assess the adequacy of the DD's policies, procedures, and processes to manage the risks associated with escrow services, and management's ability to implement effective due diligence, monitoring, and reporting systems.*

Note: *Department examiners should review the DD's escrow service activities in addition to traditional Trust and Asset Management Services processes based on the DD's activity to form an overall view of the DD's risk-based approach.*

Escrow accounts are a form of trust that has gained popularity in the digital asset space. They usually involve a third-party administrator that receives and, after specified conditions are met, disburses assets from the DD's customer (trustor) to another counterparty (trustee).

Illustrative Example[325]



Traditional escrow accounts are used in the buying and selling of real estate or other assets to address concerns of trust between the parties, where a third-party holds funds during the course of a transaction or contractual obligation subject to terms being met. Within this context, a DD is permitted to offer similar services, functioning as the trusted intermediary to connect a purchase (trustor) with a seller (trustee), holding on to the assets. DDs should have policies and procedures to document a list of permissible digital assets for escrow as well as any additional mitigating controls as appropriate based on the digital asset type.

[325] Note the example provided represents a depiction of an "escrow via direct payment." As part of its review processes, the Department should review the DD's documentation to determine that the DD has appropriate controls based on the specific protocols it is using for its escrow services, including any counterparty risk from listed sanctions persons, or other AML/CFT or OFAC risks that may be associated with that particular method.

To satisfy Customer Identification Program (CIP) rules, an institution "is not required to search the trust, escrow, or similar accounts to screen the identities of beneficiaries, but instead is only required to screen the identity of the named accountholder." However, the CIP rule goes on to state that, based on the DD's risk assessment of a new account opened by a customer that is not an individual, the DD may need "to obtain information about" individuals with authority or control over such an account, including signatories, in order to screen the customer's identity.[326] Other jurisdictions where similar digital asset trust activity is permitted, require that proper CDD measures are in place for the trustor and trustee. For example, the Monetary Authority of Singapore notes:

> "[A] payment service provider shall perform CDD measures on the customer by identifying the settlors, trustees, the protector (if any), the beneficiaries (including every beneficiary that falls within a designated characteristics or class) and any natural person exercising ultimate ownership, ultimate control or ultimate effective control over the trust (including through a chain of control or ownership)."[327]

Further, FATF notes that "trust and company service providers" should comply with FATF Recommendations 21 and 22 which, among other things, recommend CDD be performed on all relevant parties to a transaction.[328] Similarly, the Department requires CDD to be performed on all counterparties to a digital assets escrow activity, including identifying ultimate beneficial owners related to the entities involved.

For more information on escrow services, see the DD Custody & Fiduciary Manual.

Risk Factors:

Digital assets escrow services for DDs present AML/CFT and OFAC concerns similar to traditional trust and asset management accounts, with heightened risks depending on the nature of the digital assets under escrow. Traditional concerns are primarily due to the unique relationship structures involved in trust activities, including potentially opaque legal structures of the counterparty absent mitigating controls, as well as challenges in identifying customer information and unusual activity.

When misused, escrow accounts can conceal the source and use of funds, in particular as it relates to digital assets associated with anonymity, as well as the identity of beneficial and legal owners. Customers and account beneficiaries may try to remain anonymous in order to move illicit funds or to avoid scrutiny. For example, customers may seek a certain level of anonymity by creating

---

[326] Refer to 31 CFR 1020.220(a)(2(ii)(C).

[327] See "6-5-3 Identification of Customer that is a Legal Person or Arrangement from" from Monetary Authority of Singapore's, "Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism" (March 2020).

[328] Refer to 140 from "Guidance For a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf (2019).

private investment companies (PIC),[261] offshore trusts, or other investment entities that hide the true ownership or beneficial interest of the trust. Accordingly, Department examiners should assess that DDs have clearly documented processes for responding to circumstances in which the DD cannot form a reasonable belief that it knows the true identity of a customer.[329] This includes ongoing due diligence to screen that the circumstances with the trustor or trustee relationship were initially put in place still remain accurate and up-to-date, with appropriate controls to prevent the processing of funds in the case that the customer identity cannot be verified.

Similar to high-risk fiat-based products and services such as dealing in precious metal or trade finance activities, while DDs should be attendant to digital assets escrow activity involving higher-risk goods (e.g., digital assets with lower liquidity or anonymity-enhancing features), DDs also need to be aware that goods may be over- or under-valued in an effort to evade anti-money laundering or customs regulations, or to move funds or value across national borders. For example, an escrow trustee may misrepresent the value of one end of the transaction. Alternately, escrow documents, such as invoices, may be fraudulently altered to hide the scheme. Accordingly, the DD should have robust controls with a documentation review and MIS in place to establish the legitimacy of assets under contract with identified typologies and red flags in place.

Risk Mitigation:

Management should develop policies, procedures, and processes that enable the DD to identify unusual account relationships and circumstances, questionable assets and sources of assets, and other potential areas of risk (e.g., offshore accounts, PICs, asset protection trusts (APT), agency accounts, and unidentified beneficiaries). While digital assets accounts do not require EDD in all instances, management should be alert to those situations that need additional review or research, in particular around privacy coins and AECs. Given the heightened risk associated with digital asset escrow activities, the Department takes a risk-based approach, requiring that the DD identify all counterparties in an escrow exchange, with appropriate sanctions screening to screen that the parties to the transaction, including ultimate beneficial owners, are not subject to sanctions lists at outset or upon execution of the smart contract or other escrow arrangement. Similarly, the customer should be able to clearly identify the source of any digital assets held in escrow, with the DD having digital asset analytics and attestations to screen the source of funds as appropriate.

Documentary Review of Source of Funds

DDs should have due diligence processes that include gathering sufficient information on parties to an escrow transaction, including their identities, nature of business, and source of funds. To the extent feasible, DDs should review documentation, not only for compliance with the terms of the escrow transaction itself, but also for anomalies or red flags that could indicate unusual or suspicious activity, with appropriate documentation (e.g., checklists) demonstrating such reviews.

[329] Refer to 31 CFR 1020.220(a)(2)(iii).

Refer to the *Appendix B: Money Laundering and Terrorist Financing Red Flags Associated with Digital Asset* for more information.

Circumstances Warranting Enhanced Due Diligence

Management should assess account risk on the basis of a variety of factors, which may include:

- Type(s) of digital assets.
- Type of trust or agency account and its size.
- Types and frequency of transactions.
- Country of residence of the principals and beneficiaries, or the country where established, as well as the country associated with the source of funds.
- Accounts and transactions that are not usual and customary for the customer or for the DD.

Stringent documentation, verification, and transaction monitoring procedures should be established for accounts that management considers as higher risk, with clearly defined criteria for customer risk ratings. The list below provides examples of situations in which EDD may be appropriate based on traditional trust relationships, however, Department examiners should assess how DDs have formulated risk-based processes that identify where EDD measures may be warranted based on additional digital assets-specific risk considerations.

- DD is entering into a relationship with a new customer.
- Account principals or beneficiaries reside in a foreign jurisdiction, or the trust or its funding mechanisms are established in an "offshore" jurisdiction.
- Assets or transactions are atypical for the type and character of the customer.
- Account type, size, assets, or transactions are atypical for the DD.
- International funds transfers or virtual currency funds transfers are conducted, particularly through offshore funding sources.
- Accounts benefit charitable organizations or other nongovernmental organizations (NGO) that may be used as a conduit for illegal activities.
- Interest on lawyers' trust accounts (IOLTA) holding and processing significant dollar amounts.
- Account assets that include personal investment companies ("PICs").
- PEPs are parties to any accounts or transactions.

4.3.1. Digital Assets Escrow Services — Examination Procedures

Objective. *Review/assess the adequacy of the DD's policies, procedures, and processes to manage the risks associated with escrow services, and management's ability to implement effective due diligence, monitoring, and reporting systems.*

Procedure	Comments
1. Review the policies, procedures, and processes related to the DD's digital assets escrow services. Evaluate the adequacy of the policies, procedures, and processes given the DD's proposed or existing escrow activities (including what types of digital assets are permitted) and the risks they present. Assess whether the controls are adequate to reasonably protect the DD from money laundering and terrorist financing.	
2. Review the DD's procedures for gathering additional identification information about the settlor, grantor, trustee, or other persons with authority to direct a trustee, and who thus have authority or control over the account, in order to establish the true identity of the customer.	
3. From a review of MIS and internal risk rating factors, determine whether the DD effectively identifies and monitors digital assets escrow activities, particularly those that pose a higher risk for money laundering.	
4. Determine how the DD includes digital assets escrow relationships in a DD-wide or, if appropriate, DD-wide AML/CFT aggregation systems. These measures should include a unified customer view for how the customer's escrow services activity aligns with the stated purpose of the account taking account of other services that the customer currently is using.	

Procedure	Comments
5. Determine whether the DD's system for monitoring digital assets escrow activity for suspicious activities, and for reporting of suspicious activities, is adequate given the DD's size, complexity, location, and types of customer relationships.	
6. Determine whether the DD has in place sufficient due diligence processes that include gathering sufficient information on parties to an escrow transaction, including their identities, nature of business, and sources of funding.	
7. Determine whether the DD's system for screening of digital assets escrow activity for potential sanctions evasion, and for reporting of sanctioned activity, is adequate given the DD's size, complexity, location, and types of customer relationships. This should include a review of policies and procedures to identify the end-to-end process flows for types of escrow services offered, and sanctions screening conducted through each stage of the escrow activity against up-to-date sanctions lists.	
Transaction Testing	
8. On the basis of the DD's risk assessment of its digital asset escrow relationships, as well as prior examination and audit reports, select a sample of escrow services relationships. To the degree that there is identified higher-risk activity, consider a sample-based approach of those customers. Include relationships with grantors and co-trustees, if they have authority or control, as well as any higher-risk assets included as part of escrow activity. From the sample selected, perform the following examination procedures: • Review account opening documentation, including the CIP, to	

Procedure	Comments
ensure that adequate due diligence has been performed and that appropriate records are maintained. • Review account statements and, as necessary, specific transaction details. Compare expected transactions with actual activity. • Determine whether actual activity is consistent with the nature of the customer's business and the stated purpose of the account. • Identify any unusual or suspicious activity.	
9. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with digital asset escrow services.	

4.4. Stablecoin Networks — Overview

Objective. *Assess the adequacy of the DD's policies, procedures, and processes to manage the risks associated with stablecoin networks and management's ability to implement effective due diligence, monitoring, and reporting systems.*

Innovative payment instruments (e.g., "stablecoins")[330] are a type of digital asset with built-in mechanisms designed to reduce price volatility. While other digital assets have historically had significant price fluctuations, the relative stability of some stablecoins facilitates their everyday use as a store of value or as a means for clearing and settling.

For more information on innovative payment instruments, including stablecoins, see *Section 4.5. Liquidity Risk - Reserve Management* of the DD Payment Systems Risk Manual.

Design Considerations around Stablecoins

As identified in the *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, the use of a stablecoin or stablecoin network presents similar AML/CFT and OFAC risks that other large scale value transfer systems pose, including the "potential for anonymity, global reach, and layering of illicit funds." Furthermore, FATF notes that "one of the main use-cases" of stablecoins is their ability to facilitate more efficient cross-border transfers, elevating the digital asset risks associated with ML/TF and sanctions evasion.[331] Stablecoin regulation and oversight is not standardized, resulting in some stablecoins falling outside the regulatory perimeter,[332] thereby making users and the broader landscape vulnerable to financial crime risks. Furthermore, data from blockchain analytics providers points to outsized sanctions risks associated with stablecoins based on the overall value of assets held in OFAC-sanctioned wallets.[333]

Existing guidance around stablecoin projects notes that authorities should address potential ML/TF risks "in an ongoing and forward-looking manner" prior to launch particularly where peer-to-peer

[330] The Financial Stability Board defines a stablecoin as "as a crypto-asset designed to maintain a stable value relative to another asset (typically a unit of currency or commodity) or a basket of assets. These may be collateralised by fiat currency or commodities or supported by algorithms. The term is used to describe a particular set of digital assets with certain design characteristics or stated objectives, but the use of this term should not be construed as any endorsement or legal guarantee of the value or stability of these tokens." See FSB, "Regulatory issues of stablecoins" (October 18, 2019).

[331] FATF, "FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins" (June 2020).

[332] President's Working Group on Financial Markets, FDIC, and OCC, "Report on Stablecoins" (November 2021).

[333] Elliptic, "Crypto Addresses Holding NFTs Worth $532k are Among the Latest Sanctioned by OFAC" (November 2021).

transaction usage is permissible, given the difficulties to mitigate risks once launched.[334] As part of its risk evaluation, the Department considers the stablecoin's design across a range of factors, including:

- **Network Access** – Network access design plays a critical role in determining the inherent ML/TF and OFAC risk of a stablecoin network. Private stablecoin networks, achieved through underlying permissioned blockchains or other controls, enable network operators to control access to the network. With access criteria in place, a wholesale private blockchain network could limit transactions to approved legal entities, while retail private blockchain networks could require KYC controls for network participants. Critically, in both instances, network participants could be identified, assuming sufficient controls are in place.

  As a contrast to private stablecoin networks with defined access criteria, "public, permissionless, and decentralized ledgers"[335] pose greater ML/TF and sanctions risk. Depending on the network design (and the degree to which a stablecoin network is publicly accessible), unknown parties will likely access the network through unhosted wallets, requiring additional controls and screening mechanisms.

- **Anonymity Enhancing Features –** Similar to certain existing digital assets, (such as the so-called "privacy coins") stablecoin networks have the potential for anonymity enhancing features to be built into the protocol of their underlying blockchain. Anonymity enhancing features (such as non-interactive zero-knowledge proofs, stealth addresses, "coinjoin" functionality, etc.) can be used to obfuscate transaction details such as the originator, beneficiary and the transaction amount, hindering a DD's ability to conduct transaction tracing, transaction monitoring, and counterparty identification. These heightened risks posed by anonymity-enhancing features are compounded when coupled with public permissionless networks.

- **On-Off Ramp (Issuance/Redemption) –** For collateralized stablecoins, the stablecoin's network design must also address how issuance and redemption occurs and if the stablecoin is accessible through digital asset exchanges. Stablecoin networks where the stablecoin is collateralized by fiat or commodities will likely have a legal entity or a set of established legal entities to act as the Stablecoin Network Administrator (parties approved to issue and redeem stablecoins). Stablecoin Network Administrators will effectively be permitted to perform on-off-ramping services in exchange for the collateralized asset (i.e., issuance/redemption). In practice, attributes associated with issuance and on-ramp (e.g., single versus multiple redemption authorities which could span different jurisdictions) impact the overall ML/TF and sanctions risks. Additionally, the stablecoin network must

[334] FATF, "FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins" (June 2020).

[335] Ibid

address whether the stablecoin could be available through digital asset exchanges that would enable on-off ramping without issuing or redeeming existing stablecoins.

Ownership / Development / Participation in Stablecoin Network

As part of its AML/CFT and OFAC risk evaluation, examiners should consider the role that the DD plays within the stablecoin network. As FinCEN has clarified, AML/CFT [and OFAC] obligations depend on the facts and circumstances, and "differences in similar business models may lead to different regulatory applications." Additionally, a person engaged in more than one type of business model could be subject to more than one type of regulatory obligation or exemption. For example, a developer or seller of either a software application or a new virtual currency platform may be exempt from BSA obligations associated with creating or selling the application or virtual currency platform, but may still have BSA obligations as a money transmitter if the seller or developer also uses the new application to engage as a business in accepting and transmitting currency, funds, or value that substitutes for currency, or uses the new platform to engage as a business in accepting and transmitting the new virtual currency. Likewise, an exemption may apply to a person performing a certain role in the development or sale of a software application, while a different person using the same application to accept and transmit currency, funds, or value that substitutes for currency would be still subject to BSA obligations.[336]

Accordingly, DDs should clearly document their roles and responsibilities based on all the functions that they perform (e.g., as a network operator, participant, or otherwise). In the absence of a centralized control function, they should demonstrate how their participation in such an activity remains consistent with AML/CFT and OFAC obligations.

Risk Mitigation:

Where DDs issue stablecoins or participate in stablecoin networks, they should have policies, procedures, and processes sufficient to manage the related AML/CFT and OFAC risks as required under the BSA and implementing regulations, as well as relevant payment network.[337] As FinCEN has summarized: "a person that chooses to set up a transaction system that makes it difficult to comply with existing regulations may not invoke such difficulty as a justification for non-compliance or as a reason for preferential treatment."[338] These controls should also include documented processes and workflows to describe design [and deployment] considerations, and how the stablecoin network is able to meet existing AML/CFT and OFAC requirements, including

[336] FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 2019).

[337] Refer to the DD Payments Systems Risk Procedures for more information.

[338] FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 2019). See "Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets" (October 2019) for additional commentary on BSA considerations based on the type of digital asset.

the ability to identify counterparties for screening purposes prior to launch. Key considerations include:

- **Ability to screen customer identity.** Given risks around anonymity and the potential for public, permissionless, and decentralized ledgers, stablecoins present further challenges. Where a DD offers stablecoins, there should be a means to identify the customer and counterparty and maintain transaction records. The stablecoin network should have robust controls to account for customer identity, taking into account the factors described above, e.g., through a network participant questionnaire, that demonstrates that a network participants has appropriate AML/CFT and sanctions standards.[339] Additionally, if a stablecoin network is publicly accessible, the stablecoin network should have controls in place to ensure that network participants must verify their identify and complete other appropriate due diligence in order to be issued or redeem an asset.

- **Ability to conduct transaction monitoring.** The design of a stablecoin network may hinder the ability to conduct reviews for unusual activity. For example, stablecoins that allow for peer-to-peer transfers reduce the ability to conduct appropriate transaction monitoring. Particularly if the stablecoin has a global reach and could function as a vehicle for cross-border payments, the stablecoin's design could reduce the ability to identify instances or patterns of unusual activity. Stablecoin networks should be supported by blockchain analytics to facilitate the identification of unusual activity.

- **Ability to conduct screening of network participants.** Depending on the factors above (e.g., whether access criteria require network participant onboarding) a stablecoin could limit its exposure to network participants explicitly. The DD should have clearly documented policies and procedures evidencing how it conducts screening against sanctions lists and as warranted due diligence consistent with fiat-based transaction flows that operate similarly, taking into account risks associated with permissions and access criteria.[340] These controls should take into account the role that the DD places within the stablecoin network, network accessibility, and global reach of the stablecoin network.

- **Ability to define restrictions and permissible usage.** At a minimum, DDs that operate stablecoins as a network administrator or network operators should have controls in place to demonstrate how they would not run counter to OFAC-listed jurisdictional requirements and other applicable restricted activity. For example, in a private network there could be enforcement mechanisms up to and including removal from the network in the event a network operator does not meet certain standards. Similarly, in a more public network,

[339] See, for example, the International Securities Services Administration's "ISSA Financial Crime Compliance Sample Questionnaire" and the Wolfsberg Group's "Correspondent Banking Due Diligence Questionnaire" as two industry standards for AML/CFT reliance.

[340] See the DD Payment Systems Risk Procedures for more information.

there could be conditions set forth through the network's design or through off-chain processes create appropriate safeguards.

- **Blocking/Freezing and forfeiture of funds.** Depending on the DD's role within the network, the DD should have policies, processes, and procedures in place to block/freeze funds. Given the fungibility of certain stablecoins (e.g., inclusion of stablecoins in omnibus accounts), the network administrator should have clear processes in place to address law enforcement requests for the blocking or freezing of funds for any stablecoins that it issues.

- **Regulatory Approval.** Where a DD serves as an issuer/administrator of stablecoins, it should ensure that it obtains the appropriate regulatory approval prior to launch. Where the DD lists or otherwise supports certain stablecoins, it should review as part of its asset due diligence process which capabilities are built into the asset to ensure regulatory compliance and whether the stablecoin project has obtained the appropriate regulatory approval(s) (e.g., registration with FinCEN).

4.4.1. Stablecoin Networks — Examination Procedures

Objective. *Assess the adequacy of the DD's policies, procedures, and processes to manage the risks associated with stablecoin networks, and management's ability to implement effective due diligence, monitoring, and reporting systems.*

Procedure	Comments
Note – Department examiners should evaluate each stablecoin network on a standalone basis against key FFIEC considerations (e.g., CIP, Suspicious Activity Reporting, etc.). These procedures pertain to issues specific to stablecoin networks and are not intended to replace federal requirements. Per FinCEN: "a person who is engaged in more than one type of business model at the same time may be subject to more than one type of regulatory obligation or exemption."[341]	
1. Review the policies, procedures, and processes related to stablecoin networks. Evaluate the adequacy of the policies, procedures, and processes given the DD's stablecoin network activities and the risks they present. Assess whether the controls are adequate to reasonably protect the DD from money laundering and terrorist financing.	
2. Review the due diligence undertaken by the DD regarding network participants and persons issuing or redeeming assets. Assess whether existing onboarding and ongoing oversight programs are reasonably satisfactory to protect the DD.	
3. Review the DD's procedures regarding access criteria.	
4. From a review of MIS and internal risk rating factors, determine whether the DD effectively identifies and monitors stablecoin network relationships, particularly those that pose a higher risk for money laundering.	
5. Determine whether the DD's stablecoin network governance for node operators and	

[341] FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 2019).

Procedure	Comments
other persons responsible for the maintenance, development or operation of the network includes an agreement or a contract describing each party's responsibilities and other relationship details, such as the products and services provided. At a minimum, the contract should consider each party's: • AML/CFT and OFAC compliance requirements; • customer base; • due diligence procedures; and • network obligations.	
6. Determine whether the DD's system for monitoring stablecoin network participant relationships for suspicious activities, and for reporting of suspicious activities, is adequate given the DD's size, complexity, location, and types of customer relationships.	
7. If appropriate, for additional guidance refer to the core examination procedures in the *2.4. Assess the OFAC Compliance Program* section.	
Transaction Testing	
8. On the basis of the DD's risk assessment of its stablecoin network relationships, as well as prior examination and audit reports, select a sample of higher-risk stablecoin network relationships or customers with access to blockchain ledger, depending on the stablecoin network's design. From the sample selected, perform the following examination procedures: • Review screening documents, especially at asset issuance or redemption, including the CIP, to ensure that adequate due diligence has been performed and that appropriate records are maintained.	

Procedure	Comments
• Review account statements and, as necessary, specific transaction details. Compare expected transactions with actual activity. • Determine whether actual activity is consistent with the nature of the customer's business and the stated purpose of the account. • Identify any unusual or suspicious activity.	
9. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes related to stablecoin risk controls.	

4.5. Virtual Currency Automated Teller Machines Owners or Operators – Overview

Objective. *Evaluate the DD's policies, procedures, and processes to assess, manage, and mitigate potential risks associated with customers who are virtual currency automated teller machines (ATMs) operators. Evaluate the DD's compliance with regulatory and registration requirements, such as customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, currency transaction reporting, and suspicious activity reporting with respect to these customers. Examiners are reminded that virtual currency ATM operators are considered MSBs and are required to comply with all applicable MSB BSA requirements, including registering with FinCEN (and state-by-state money transmitter license requirements, as applicable).*

Note: *This section focuses on ATMs as it applies to virtual currencies. For traditional fiat-based ATMs, Department examiners should review the FFIEC AML Manual's "Risks Associated with Money Laundering and Terrorist Financing – Independent Automated Teller Machine Owners and Operators" section.*

Virtual Currency ATMs (or "kiosks" or "crypto ATMs") offer fast and convenient access to virtual currencies by facilitating the buying, selling, and exchanging of digital assets, as well as the conversion of digital assets to fiat cash and, in some cases, vice versa. Per a Government Accountability Office report, "[virtual currency] kiosks are rapidly increasing in the U.S., growing from about 560 in January 2017 to over 22,600 as of September 1, 2021."[342]

Examiners, however, should be aware that virtual currency kiosks may pose heightened ML/TF risks by virtue of their unique ability to facilitate cash placement and exchange into digital assets, and, in the case of bidirectional virtual currency kiosks, their ability to facilitate digital asset off-ramping into cash, in some instances with limited due diligence standards.

Risk Factors

FinCEN specifically highlighted red flags associated with unregistered or illicitly operating virtual currency kiosks, noting that these kiosks often try to knowingly evade BSA requirements, including by facilitating structuring (money laundering) of transactions and failing to comply with CIP and other KYC requirements.[343] In guidance published in October 2020, the DOJ stated that "cryptocurrency kiosk operators—also considered MSBs in the United States—often do not comply with regulations requiring the implementation of AML/CFT programs, including identification and reporting of suspicious transactions, despite the fact that such kiosks have been linked to illicit use by drug dealers, credit card fraud schemers, prostitution rings, and unlicensed

[342] Government Accountability Office, "Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking" (December 2021).

[343] FinCEN, "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 2019).

virtual asset exchangers."[344] Additionally, kiosk operators are not required to report their kiosks' specific locations, therefore making it difficult for law enforcement to identify kiosks in high-risk jurisdictions for financial crimes, and enforce compliance with MSB BSA registration[345] and reporting requirements.[346] The ability for customers using virtual currency kiosks to convert digital assets into fiat cash—and in the case of some kiosks, converting fiat cash into digital assets—poses a significant ML/TF risk. For example, criminals can deposit large sums of cash from illegal drug proceeds into a kiosk to convert these funds into digital assets and make it challenging for law enforcement to track and trace the funds and identify the illicit actors.[347]

Risk Mitigation

Understanding a customer's risk profile enables the DD to apply appropriate policies, procedures, and processes to manage and mitigate risk, and comply with AML/CFT regulatory requirements. Like all DD accounts, those held by virtual currency ATM owner or operator customers are subject to AML/CFT regulatory requirements. These include requirements related to customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, currency transaction reporting, and suspicious activity reporting. Consistent with a risk-based approach, the level and type of CDD should be commensurate with the risks presented by the customer relationship.

DDs must have appropriate risk-based procedures for conducting ongoing CDD to understand the nature and purpose of customer relationships and to develop a customer risk profile. Examiners should assess how a DD evaluates virtual currency ATM owner or operator customers according to their particular characteristics to determine whether the DD can effectively mitigate the risk these customers may pose, obtain more customer information for those customers with a higher customer risk profile and may collect less information for customers with a lower customer risk profile, as appropriate. Given the rise of bulk cash smuggling and other crimes involving both fiat and digital assets (e.g., through the use of virtual asset kiosks),[348] examiners should also evaluate whether the DD has appropriate controls in place for the monitoring and reporting of such activity and transactions. Furthermore, examiners should evaluate whether the DD operates a kiosk or has customers that operate a kiosk, and if they are in compliance with all applicable MSB BSA registration (i.e., registering as an MSB with FinCEN) and reporting requirements, including providing accurate kiosk locations upon request to help law enforcement better identify the source of illicit transactions, such as human and drug trafficking, as well as verifying and collecting

---

[344] Department of Justice: Attorney General's Cyber-Digital Task Force, "DOJ released 'Cryptocurrency: An Enforcement Framework'" (October 2020).

[345] From 2018 to 2020, the number of known unregistered virtual currency kiosks has increased significantly.

[346] Government Accountability Office, "Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking" (December 2021).

[347] Ibid

[348] U.S. Treasury, "National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing" (March 2022).

customer information on certain transactions, and maintaining an adequate AML program more broadly.[349]

Examiner Evaluation

Examiners should evaluate the DD's processes for assessing risks associated with customers that are virtual currency ATM owners or operators. Examiners should determine whether the DD's internal controls are designed to ensure ongoing compliance and are commensurate with the DD's risk profile. Examiners should also determine whether internal controls manage and mitigate ML/TF and other illicit financial activity risks for virtual currency ATM owner and operator customers. Examiners may conduct this assessment when evaluating the DD's compliance with regulatory requirements, such as customer identification, CDD, and suspicious activity reporting. More information can be found in the *Assessing the AML/CFT Compliance Program – AML/CFT Internal Controls* and *Assessing Compliance with BSA Regulatory Requirements* sections of this Manual.

[349] Government Accountability Office, "Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking" (December 2021).

4.5.1. Virtual Currency Automated Teller Machines Owners or Operators Examination And Testing Procedures

Objective. *Evaluate the DD's policies, procedures, and processes to assess, manage, and mitigate potential risks associated with customers who are virtual currency ATM operators. Evaluate the DD's compliance with regulatory and registration requirements, such as customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, currency transaction reporting, and suspicious activity reporting with respect to these customers. Examiners are reminded that virtual currency ATM operators are considered MSBs and are required to comply with all applicable MSB BSA requirements, including registering with FinCEN (and state-by-state money transmitter license requirements, as applicable).*

The following examination and testing procedures are intended to be a subset of a broader review of compliance with Bank Secrecy Act/anti-money laundering (AML/CFT) regulations, such as customer identification, customer due diligence (CDD), beneficial ownership, currency transaction reporting, and suspicious activity reporting. Not all of the examination and testing procedures will apply to every DD or be used during every examination.

Procedure	Comments
1. Determine whether the DD has developed and implemented appropriate, written risk-based procedures for conducting ongoing CDD for all customers, including virtual currency automated teller machine (ATM) owner or operator customers, and that these procedures enable the DD to: • Understand the nature and purpose of the customer relationship in order to develop a customer risk profile. • Conduct ongoing monitoring: o for the purpose of identifying and reporting suspicious transactions, and o on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers. • Use customer information and the customer risk profile to understand the types of transactions in which a particular customer would be expected to engage, and to establish a baseline against which suspicious transactions are identified.	
2. Determine whether the DD, as part of the overall CDD program, has effective processes to develop customer risk profiles that identify the specific risks	

Procedure	Comments
of individual customers including, as appropriate, virtual currency ATM owner or operator customers.	
3. Determine whether the DD has policies, procedures, and processes to identify customers that may pose higher risk for money laundering, terrorist financing (ML/TF), and other illicit financial activities, which may include virtual currency ATM owner or operator customers. Policies, procedures, and processes generally include whether and when, based on risk, it is appropriate to obtain and review additional customer information, including guidance for resolving issues when insufficient, inaccurate, or unverifiable information is obtained. Determine whether the risk-based CDD/EDD policies, procedures, and processes are commensurate with the DD's ML/TF and other illicit financial activity risk profile.	
4. Determine whether the DD's system for monitoring virtual currency ATM owner or operator customer accounts for suspicious activities, and for reporting suspicious activities, is adequate given the DD's risk profile.	
5. Consider whether the DD's policies, procedures, and processes adequately address the preparation, filing, and retention of currency transaction reports for virtual currency ATM owner or operator customers.	

Procedure	Comments
6. Determine if performing risk-focused testing is appropriate based on the review of a risk assessment, prior examination reports, other examination information, or a review of the DD's audit findings. If risk-focused testing is appropriate, select a sample of virtual currency ATM owner or operator customer relationships and request applicable documentation to perform risk-focused testing. From the sample selected, perform the following examination procedures: • Determine whether the DD collects appropriate information to understand the nature and purpose of customer relationships, and to evaluate such customers according to their particular characteristics when assessing whether the DD can effectively mitigate the potential risk those customers may pose. • Determine whether the DD effectively incorporates customer information, including beneficial ownership information for legal entity customers, into the customer risk profile. • Review transaction activity for selected customer relationships and, if necessary, request and review specific transactions and transaction monitoring documentation to determine whether the DD has identified and reported any suspicious activity.	
7. Based on examination and testing procedures completed, form a conclusion about the adequacy of policies, procedures, and processes associated with virtual currency ATM owner or operator customers.	
8. Determine whether the DD has policies, procedures, and processes in place to ensure virtual currency kiosk customers are in compliance with MSB BSA requirements, including verifying registration with FinCEN, reviewing the virtual currency kiosk customer's AML/CFT and OFAC programs, and assessing the adequacy of their controls.	

4.6. Politically Exposed Persons – Overview

Objective. *Evaluate the DD's policies, procedures, and processes to assess, manage, and mitigate potential risks associated with foreign individual customers who the DD has designated as politically exposed persons (PEPs). Evaluate the DD's compliance with regulatory requirements, such as customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, and suspicious activity reporting with respect to these customers. Examiners are reminded that there are no Bank Secrecy Act (BSA) regulations specific to foreign individual customers who the DD has designated as PEPs.*

Bank Secrecy Act/Anti-Money Laundering (AML/CFT) regulations do not define the term Politically Exposed Person (PEP), and the term should not be confused with "senior foreign political figure" (SFPF), a subset of PEP. The term PEP is commonly used in the financial industry to refer to foreign individuals who are or have been entrusted with a prominent public function, as well as to their immediate family members and close associates.

Examiners are reminded that no specific customer type automatically presents a higher risk of money laundering, terrorist financing (ML/TF), or other illicit financial activity. Further, DDs that operate in compliance with applicable AML/CFT regulatory requirements and reasonably manage and mitigate risks related to the unique characteristics of customer relationships are neither prohibited nor discouraged from providing banking services to foreign individuals who the DD may consider to be PEPs (referred to in this section as "DD-identified PEPs").

Risk Factors

DD-identified PEP customers present varying levels of ML/TF and other illicit financial activity risks, and the potential risk to a DD depends on the presence or absence of numerous factors. Not all DD-identified PEP customers pose the same risk, and not all DD-identified PEP customers are automatically higher risk. By virtue of their public position or relationships, some DD- identified PEPs may present a risk higher than other customers by having access to funds that may be the proceeds of corruption or other illicit activity. Some foreign individuals who are DD- identified PEPs have used DDs as conduits for their illegal activities, including corruption, bribery, ML/TF, and other illicit financial activity. The potential risk to the DD depends on the facts and circumstances specific to the customer relationship, such as transaction volume, type of activity, and geographic locations.

DD-identified PEPs with a limited transaction volume, a low-dollar deposit account with the DD, known legitimate sources of funds, access only to products or services subject to specific terms and payment schedules, or a limited number of accounts with which the DD-identified PEP is associated, could reasonably be characterized as having lower customer risk profiles.

Risk Mitigation

Understanding a customer's risk profile enables the DD to apply appropriate policies, procedures, and processes to manage and mitigate risk and comply with AML/CFT regulatory requirements.

Like all DD accounts, those held by DD-identified PEPs or associated with DD-identified PEPs are subject to AML/CFT regulatory requirements. These requirements are related to customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, and suspicious activity reporting. However, there is no AML/CFT regulatory requirement or supervisory expectation for DDs to have unique or additional customer identification requirements or CDD steps for any particular group or type of customer.

Consistent with a risk-based approach, the level and type of CDD should be commensurate with the risks presented by the customer relationship. The CDD rule does not require a DD to screen for or otherwise determine whether a customer or beneficial owner of a legal entity customer may be considered a PEP. A DD may choose to determine whether a customer is a PEP at account opening if the DD determines the information is necessary to develop a customer risk profile. Further, the DD may conduct periodic reviews with respect to DD-identified PEPs as part of, or in addition to, the required ongoing risk-based monitoring to maintain and update customer information.

DDs must have appropriate risk-based procedures for conducting ongoing CDD to understand the nature and purpose of customer relationships, and to develop a customer risk profile. Examiners should assess how a DD evaluates DD-identified PEP customers according to their particular characteristics to determine whether the DD can effectively mitigate the potential risk these customers may pose. Consistent with a risk-based approach for conducting ongoing CDD, a DD should typically obtain more customer information for those customers with a higher customer risk profile and may collect less information for customers with a lower customer risk profile, as appropriate.

The information collected to create a customer risk profile should also assist DDs in conducting ongoing monitoring to identify and report suspicious activity. Moreover, performing an appropriate level of ongoing CDD commensurate with the customer's risk profile assists the DD in determining whether a customer's transactions are suspicious.

Based on the customer risk profile, the DD may consider obtaining, at account opening (and throughout the relationship), more customer information in order to understand the nature and purpose of the customer relationship. The following information may be useful for a DD in understanding the nature and purpose of the customer relationship and, therefore, in determining the ML/TF and other illicit financial activity risk profile of DD-identified PEP customers:

- The type of products and services used.
- The volume and nature of transactions.
- Geographies associated with the customer's activity and domicile.
- The customer's official government responsibilities.
- The level and nature of the customer's authority or influence over government activities or officials.
- The customer's access to significant government assets or funds.

DDs may leverage existing processes for assessing geographically specific ML/TF, corruption, and other illicit financial activity risks when developing the customer risk profile. Existing processes may also take into account the jurisdiction's legal and enforcement frameworks, including ethics reporting and oversight requirements. For a DD-identified PEP who is no longer in active government service, DDs may also consider the time that the customer has been out of office and the level of influence he or she may still hold as factors in the customer risk profile. When developing customer risk profiles and determining when to collect additional customer information, and what to collect, DDs may take into account such factors as the customer's public office or position of public trust (or that of the customer's family members or close associates), as well as any indication that the DD-identified PEP misuses his or her authority or influence for personal gain. Refer to the *Customer Due Diligence* and *Suspicious Activity Reporting* sections for more information.

Examiner Evaluation

Examiners should evaluate the DD's processes for assessing risks associated with customers that are DD-identified PEPs. Examiners should determine whether the DD's internal controls are designed to ensure ongoing compliance and are commensurate with the DD's risk profile. Examiners should also determine whether internal controls manage and mitigate ML/TF and other illicit financial activity risks for DD-identified PEPs. Examiners may conduct this assessment when evaluating the DD's compliance with regulatory requirements such as customer identification, CDD, and suspicious activity reporting. More information can be found in the *Assessing the AML/CFT Compliance Program - AML/CFT Internal Controls* and *Assessing Compliance with BSA Regulatory Requirements* sections of this Manual.

4.6.1. Politically Exposed Persons Examination and Testing Procedures

Objective. *Evaluate the DD's policies, procedures, and processes to assess, manage, and mitigate potential risks associated with foreign individual customers who the DD has designated as politically exposed persons (PEPs). Evaluate the DD's compliance with regulatory requirements, such as customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, and suspicious activity reporting, with respect to these customers. Examiners are reminded that there are no Bank Secrecy Act (BSA) regulations specific to foreign individual customers who the DD has designated as PEPs.*

The following examination and testing procedures are intended to be a subset of a broader review of compliance with Bank Secrecy Act/anti-money laundering (AML/CFT) regulations, such as customer identification, customer due diligence (CDD), beneficial ownership, and suspicious activity reporting. Not all of the examination and testing procedures will apply to every DD or will be used during every examination.

Procedure	Comments
1. Determine whether the DD has developed and implemented appropriate, written risk-based procedures for conducting ongoing CDD for all customers, including DD-identified PEP customers, and that these procedures enable the DD to: • Understand the nature and purpose of the customer relationship in order to develop a customer risk profile. • Conduct ongoing monitoring: o for the purpose of identifying and reporting suspicious transactions; and o on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers. • Use customer information and the customer risk profile to understand the types of transactions in which a particular customer would be expected to engage, and to establish a baseline against which suspicious transactions are identified.	

Procedure	Comments
2. Determine whether the DD, as part of the overall CDD program, has effective processes to develop customer risk profiles that identify the specific risks of individual customers including, as appropriate, DD-identified PEP customers.	
3. Determine whether the DD has policies, procedures, and processes to identify customers that may pose higher risk for money laundering, terrorist financing (ML/TF), and other illicit financial activities, which may include DD-identified PEP customers. Policies, procedures, and processes generally include whether and when, based on risk, it is appropriate to obtain and review additional customer information, including guidance for resolving issues when insufficient, inaccurate, or unverifiable information is obtained. Determine whether the risk-based CDD policies, procedures, and processes are commensurate with the DD's ML/TF and other illicit financial activity risk profile.	
4. Determine whether the DD's system for monitoring DD-identified PEP customer accounts for suspicious activities, and for reporting suspicious activities, is adequate given the DD's risk profile.	
5. Determine if performing risk-focused testing is appropriate based on the review of a risk assessment, prior examination reports, other examination information, or a review of the DD's audit findings. If risk-focused testing is appropriate, select a sample of DD-identified PEP relationships and request applicable documentation to perform risk-focused testing. From the sample selected, perform the following examination procedures: • Determine whether the DD collects appropriate information to understand	

Procedure	Comments
the nature and purpose of customer relationships, and to evaluate such customers according to their particular characteristics when assessing whether the DD can effectively mitigate the potential risk those customers may pose. • Determine whether the DD effectively incorporates customer information, including beneficial ownership information for legal entity customers, into the customer risk profile. • Review transaction activity for the selected customer relationships and, if necessary, request and review specific transactions and transaction monitoring documentation to determine whether the DD has identified and reported any suspicious activity.	
6. Based on examination and testing procedures completed, form a conclusion about the adequacy of policies, procedures, and processes associated with DD-identified PEP customers.	

4.7. Charities and Nonprofit Organizations – Overview

Objective. *Evaluate the DD's policies, procedures, and processes to assess, manage, and mitigate potential risks associated with customers that are charities and other nonprofit organizations (NPOs). Evaluate the DD's compliance with regulatory requirements such as customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, and suspicious activity reporting with respect to these customers. Examiners are reminded that there are no Bank Secrecy Act (BSA) regulations specific to customers that are charities and other NPOs.*

Many charities and other nonprofit organizations (NPOs) pursue activities that are intended to serve the public good and provide various services, including building communities, relieving suffering, providing life-saving assistance, and helping developing nations. The federal banking agencies and FinCEN have recognized that it is vital for legitimate charities and other NPOs to have access to financial services, including the ability to transmit funds in a timely manner.

Examiners are reminded that no specific customer type automatically presents a higher risk of money laundering, terrorist financing (ML/TF), or other illicit financial activity. Further, DDs that operate in compliance with applicable Bank Secrecy Act/anti-money laundering (AML/CFT) regulatory requirements and reasonably manage and mitigate risks related to the unique characteristics of customer relationships are neither prohibited nor discouraged from providing financial services to charities and other NPOs.

Risk Factors

Charity and other NPO customers present varying levels of ML/TF and other illicit financial activity risks, and the potential risk to a DD depends on the presence or absence of numerous factors. Examiners are reminded that the U.S. government does not view the charitable sector as a whole as presenting a uniform or unacceptably high risk of being used or exploited for ML/TF or sanctions violations. The potential risk to the DD depends on the facts and circumstances specific to the customer relationship, such as transaction volume, type of activity, and geographic locations.

The ML/TF risk for charity and other NPO customers can also vary depending on the operations, activities, leadership, and affiliations of the organization. For example, U.S. charities that operate and provide funds solely to domestic recipients generally present lower ML/TF risk. However, those U.S. charities that operate abroad, or that provide funding to, or have affiliated organizations in conflict regions can face potentially higher ML/TF risks. Moreover, in the context of digital assets, certain token projects may take the form of a foundation that is organized as either a charity or NPO. In such instances, FFIEC requirements around charities and NPOs additionally apply, even where the activity of such digital asset entities, differs in some respects from that of traditional charities and NPOs.

Risk Mitigation

Understanding a customer's risk profile enables the DD to apply appropriate policies, procedures, and processes to manage and mitigate risk and otherwise comply with AML/CFT regulatory requirements. Like all DD accounts, those held by charity and other NPO customers are subject to AML/CFT regulatory requirements. These include requirements related to customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, and suspicious activity reporting. However, there is no AML/CFT regulatory requirement or supervisory expectation for DDs to have unique or additional customer identification requirements or CDD steps for any particular group or type of customer. Consistent with a risk- based approach, the level and type of CDD should be commensurate with the risks presented by the customer relationship.

DDs must have appropriate risk-based procedures for conducting ongoing CDD to understand the nature and purpose of customer relationships, and to develop customer risk profiles. Examiners should assess how a DD evaluates charity and other NPO customers according to their particular characteristics to determine whether the DD can effectively mitigate the risk these customers may pose. Consistent with a risk-based approach for conducting ongoing CDD, a DD should typically obtain more customer information for those customers with a higher customer risk profile and may collect less information for customers with a lower customer risk profile, as appropriate.

The information collected to create a customer risk profile should also assist DDs in conducting ongoing monitoring to identify and report any suspicious activity. Moreover, performing an appropriate level of ongoing CDD that is commensurate with the customer's risk profile assists the DD in determining whether a customer's transactions are suspicious.

Charities and other NPOs are also subject to federal and state reporting requirements and regulatory oversight. For example, charities report specific information annually on IRS Form 990 regarding their stated mission, programs, finances (including non-cash contributions), donors, activities, and funds sent and used abroad. Many NPOs also adhere to voluntary self-regulatory standards and controls to improve individual governance, management, and operational practice, in addition to internal controls required by donors and others.

Based on the customer risk profile, the DD may consider obtaining, at account opening (and throughout the relationship), more customer information in order to understand the nature and purpose of the customer relationship. The following information may be useful for a DD in understanding the nature and purpose of the customer relationship and in determining the ML/TF and other illicit financial activity risk profile of charity and other NPO customers:

- Purpose and nature of the charity and NPO, including mission(s), stated objectives, programs, activities, and services.
- Organizational structure, including key principals and management.
- Geographic locations served, including headquarters and operational areas, particularly in higher-risk areas where terrorist groups are most active.

- Information pertaining to the operating policies, procedures, and internal controls of the charity and NPO.
- State incorporation or registration, and tax-exempt status by the Internal Revenue Service (IRS) and required reports with regulatory authorities.
- Voluntary participation in self-regulatory programs to enhance governance, management, and operational practice.
- Financial statements, audits, and any self-assessment evaluations.
- General information about the donor base, funding sources, and fundraising methods, and, for public charities, the level of support from the general public.
- General information about beneficiaries and criteria for disbursement of funds, including guidelines/standards for qualifying beneficiaries and any intermediaries that may be involved.
- Affiliation with other charities, NPOs, foundations, governments, or groups.

Additional information that may be useful in determining the customer risk profile of a charity or other NPO is available at the U.S. Department of the Treasury's Resource Center, Protecting Charitable Organizations.

Refer to the *Customer Due Diligence* and *Suspicious Activity Reporting* sections for more information.

Examiner Evaluation

Examiners should evaluate the DD's processes for assessing risks associated with customers that are charities and NPOs. Examiners should determine whether the DD's internal controls are designed to ensure ongoing compliance and are commensurate with the DD's risk profile. Examiners should also determine whether internal controls manage and mitigate ML/TF and other illicit financial activity risks for charity and other NPO customers. Examiners may conduct this assessment when evaluating the DD's compliance with regulatory requirements, such as customer identification, CDD, and suspicious activity reporting. More information can be found in the *Assessing the AML/CFT Compliance Program - AML/CFT Internal Controls* and *Assessing Compliance with BSA Regulatory Requirements* sections of this Manual.

4.7.1. Charities And Nonprofit Organizations Examination And Testing Procedures

Objective. *Evaluate the DD's policies, procedures, and processes to assess, manage, and mitigate risks associated with customers that are charities and other nonprofit organizations (NPOs). Evaluate the DD's compliance with regulatory requirements, such as customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, and suspicious activity reporting, with respect to these customers. Examiners are reminded that there are no Bank Secrecy Act (BSA) regulations specific to customers who are charities and other NPOs.*

The following examination and testing procedures are intended to be a subset of a broader review of compliance with Bank Secrecy Act/anti-money laundering (AML/CFT) regulations, such as customer identification, customer due diligence (CDD), beneficial ownership, and suspicious activity reporting. Not all of the examination and testing procedures will apply to every DD or will be used during every examination.

Procedure	Comments
1. Determine whether the DD has developed and implemented appropriate, written risk-based procedures for conducting ongoing CDD for all customers, including charity, nonprofit organization (NPO) and digital asset foundation customers, and that these procedures enable the DD to: • Understand the nature and purpose of the customer relationship in order to develop a customer risk profile. • Conduct ongoing monitoring: o for the purpose of identifying and reporting suspicious transactions; and o on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers. (As a reminder, charity and NPO customers are only subject to the control prong of the beneficial ownership requirement, which requires the identification and verification of a single individual with significant responsibility to control, manage, or direct a legal entity customer.)	

Procedure	Comments
• Use customer information and the customer risk profile to understand the types of transactions in which a particular customer would be expected to engage, and to establish a baseline against which suspicious transactions are identified.	
2. Determine whether the DD, as part of the overall CDD program, has effective processes to develop customer risk profiles that identify the specific risks of individual customers including, as appropriate, charity and other NPO customers.	
3. Determine whether the DD has policies, procedures, and processes to identify customers that may pose higher risk for money laundering, terrorist financing (ML/TF), and other illicit financial activities, which may include certain charities and other NPOs. Policies, procedures, and processes generally include whether and when, based on risk, it is appropriate to obtain and review additional customer information, including guidance for resolving issues when insufficient, inaccurate, or unverifiable information is obtained. Determine whether the risk-based CDD policies, procedures, and processes are commensurate with the DD's ML/TF and other illicit financial activity risk profile. In particular, in the case of a digital asset foundation, determine whether the DD's policies, procedures, and processes adequately consider risks associated with the foundation, including founder anonymity and negative news associated with the foundation and/or project team.	
4. Determine whether the DD's system for monitoring charity and other NPO customer accounts for suspicious activities, and for reporting suspicious activities, is adequate given the DD's risk profile.	

Procedure	Comments
5. Determine if performing risk-focused testing is appropriate based on the review of a risk assessment, prior examination reports, other examination information, or a review of the DD's audit findings. If risk-focused testing is appropriate, select a sample of charity, NPO, and foundation customer relationships and request applicable documentation to perform risk-focused testing. From the sample selected, perform the following examination procedures: • Determine whether the DD collects appropriate information to understand the nature and purpose of customer relationships and to evaluate such customers according to their particular characteristics when assessing whether the DD can effectively mitigate the potential risk those customers may pose. • Determine whether the DD effectively incorporates customer information, including beneficial ownership information for legal entity customers, into the customer risk profile. (As a reminder, charity and NPO customers are only subject to the control prong of the beneficial ownership requirement, which requires the identification and verification of a single individual with significant responsibility to control, manage, or direct a legal entity customer.) • Review transaction activity for selected customer relationships and, if necessary, request and review specific transactions and transaction monitoring documentation to determine whether the DD has identified and reported any suspicious activity.	
6. Based on examination and testing procedures completed, form a conclusion about the adequacy of, and the DD's adherence to, its policies, procedures, and processes associated with charity and other NPO customers.	

4.8. Correspondent Accounts (Foreign) – Overview

Objective. *Assess the adequacy of the U.S. DD's systems to manage the risks associated with foreign correspondent banking and management's ability to implement effective due diligence, monitoring, and reporting systems. This section expands the earlier core review of statutory and regulatory requirements of foreign correspondent account relationships in order to provide a broader assessment of the AML risks associated with this activity.*

Foreign financial institutions maintain accounts at U.S. DDs to gain access to the U.S. financial system and to take advantage of services and products that may not be available in the foreign financial institution's jurisdiction. These services may be performed more economically or efficiently by the U.S. DD or may be necessary for other reasons, such as the facilitation of international trade. Services may include:

- Cash management services, including deposit accounts.
- International funds transfers.
- Check clearing.
- Payable through accounts.
- Pouch activities.
- Foreign exchange services.
- Overnight investment accounts (sweep accounts).
- Loans and letters of credit.
- Lines of credit.

Contractual Agreements

Each relationship that a U.S. DD has with a foreign correspondent financial institution, including a foreign digital asset exchange, custodian, etc., should be governed by an agreement or a contract describing each party's responsibilities and other relationship details (e.g., products and services provided, acceptance of deposits, clearing of items, forms of payment, and acceptable forms of endorsement). The agreement or contract should also consider the foreign financial institution's AML regulatory requirements, customer base, due diligence procedures, and permitted third-party usage of the correspondent account.

Risk Factors

Some foreign financial institutions are not subject to the same or similar regulatory guidelines as U.S. DDs; therefore, these foreign institutions may pose a higher money laundering risk to their respective U.S. DD correspondent(s). Investigations have disclosed that, in the past, foreign correspondent accounts have been used by drug traffickers and other criminal elements to launder funds. Shell companies are sometimes used in the layering process to hide the true ownership of accounts at foreign correspondent financial institutions. Because of the large amount of funds, multiple transactions, and the U.S. DD's potential lack of familiarity with the foreign correspondent financial institution's customer, criminals and terrorists can more easily conceal the

source and use of illicit funds. Consequently, each U.S. DD, including all overseas branches, offices, and subsidiaries, should closely monitor transactions related to foreign correspondent accounts. U.S. Treasury's 2022 National Risk Assessments for ML/TF and proliferation financing stated that "proliferation finance networks continue to misuse correspondent banking relationships and establish multiple front and shell companies to facilitate financial activity and conduct their trade... These networks are also increasingly exploiting the digital economy, including through the systematic mining and trading of virtual assets, and the hacking of virtual asset service providers."[350]

Without adequate controls, a U.S. DD may also set up a traditional correspondent account with a foreign financial institution and not be aware that the foreign financial institution is permitting other financial institutions, or customers to conduct transactions anonymously through the U.S. DD account (e.g., payable through accounts and nested accounts).

Nested Accounts

Nested accounts occur when a foreign financial institution gains access to the U.S. financial system by operating through a U.S. correspondent account belonging to another foreign financial institution. If the U.S. DD is unaware that its foreign correspondent financial institution customer is providing such access to third-party foreign financial institutions, these third-party financial institutions can effectively gain anonymous access to the U.S. financial system. Unacceptable nested activity and other activity of concern may be characterized by transactions to jurisdictions in which the foreign financial institution has no known business activities or interests and transactions in which the total volume and frequency significantly exceeds expected activity for the foreign financial institution, considering its customer base or asset size. U.S. DDs should also focus on nested account transactions with any entities the DD has designated as higher risk.

Risk Mitigation

U.S. DDs that offer foreign correspondent financial institution services should have policies, procedures, and processes to manage the AML/CFT risks inherent with these relationships and should closely monitor transactions related to these accounts to detect and report suspicious activities. Furthermore, DDs should develop and implement procedures that comply with 31 CFR 1010.610 for foreign correspondent accounts and ensure that the required due diligence information is collected and documented in the appropriate system of record. The level of risk varies depending on the foreign financial institution's strategic profile, including its size and geographic locations, the products and services it offers, and the markets and customers it serves. The Clearing House Association, LLC. and The Wolfsberg Group have published suggested industry standards and guidance for DDs that provide foreign correspondent banking services. When dealing with foreign correspondent account relationships, it is important for the

[350] U.S. Treasury, "National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing" (March 2022).

DD to keep in mind regulatory requirements related to special measures issued under 311 of the USA PATRIOT Act contained in the expanded overview section, "Special Measures." Additional information relating to risk assessments and due diligence is contained in the core overview section, “Foreign Correspondent Account Recordkeeping, Reporting, and Due Diligence.”

The U.S. DD’s policies, procedures, and processes should:

- Specify appropriate account-opening/on-boarding procedures, which may include minimum levels of documentation to be obtained from prospective customers; an account review and approval process that is independent of the correspondent account business line for potential higher-risk customers; and a description of circumstances when the DD will not open an account.
- Assess the risks posed by a prospective foreign correspondent customer relationship utilizing consistent, well-documented risk-rating methodologies, and incorporate that risk determination into the DD’s suspicious activity monitoring system.
- Understand the intended use and purpose of the accounts and expected account activity (e.g., determine whether the relationship will serve as a payable through account).
- Understand the foreign correspondent financial institution’s other correspondent relationships (e.g., determine whether and how nested accounts will be utilized).
- Conduct adequate and ongoing due diligence on the foreign correspondent financial institution relationships, which may include periodic site visits based on risk.
- Determine whether the foreign correspondent financial institution has in place acceptable AML compliance processes and controls.
- Ensure that appropriate due diligence standards are applied to those accounts determined to be higher risk.
- Ensure that foreign correspondent financial institution relationships are appropriately included within the U.S. DD's suspicious activity monitoring and reporting systems.
- Follow up on account activity and transactions that do not fit the foreign financial institution customer's strategic profile (i.e., transactions involving customers, industries or products that are not generally part of that foreign financial institution's customer base or market).
- Establish a formalized process for escalating suspicious information on potential and existing customers to an appropriate management level for review.
- Establish criteria for closing the foreign correspondent financial institution account.

As a sound practice, U.S. DDs are encouraged to communicate their AML-related expectations to their foreign correspondent financial institution customers. Moreover, the U.S. DD should generally understand and assess the quality of the AML controls at the foreign correspondent financial institution, including customer due diligence practices, suspicious activity identification processes, and recordkeeping documentation. They should also have an understanding of the effectiveness of the AML regime of the foreign jurisdictions in which their foreign correspondent banking customers operate.

4.8.1. Correspondent Accounts (Foreign) Examination and Testing Procedures

Objective. *Assess the adequacy of the U.S. DD's systems to manage the risks associated with foreign correspondent banking and management's ability to implement effective due diligence, monitoring, and reporting systems. This section expands the earlier core review of statutory and regulatory requirements of foreign correspondent account relationships in order to provide a broader assessment of the AML risks associated with this activity.*

Procedure	Comments
1. Review the policies, procedures, and processes related to foreign correspondent financial institution account relationships, including foreign digital asset service providers. Evaluate the adequacy of the policies, procedures, and processes. Assess whether the controls are adequate to reasonably protect the U.S. DD from money laundering and terrorist financing.	
2. From a review of MIS and internal risk-rating factors, determine whether the U.S. DD effectively identifies and monitors foreign correspondent financial institution account relationships, particularly those that pose a higher risk for money laundering.	
3. If the U.S. DD has a standardized foreign correspondent agreement, review a sample agreement to determine whether each party's responsibilities, products, and services provided, and allowable third-party usage of the correspondent account, are covered under the contractual arrangement. If the U.S. DD does not have a standardized agreement, refer to the transaction testing examination procedures.	
4. Determine whether the U.S. DD's system for monitoring foreign correspondent financial institution account relationships for suspicious activities, and for reporting suspicious activities, is adequate given the	

Procedure	Comments
U.S. DD's size, complexity, location, and types of customer relationships.	
5. If appropriate, for additional guidance refer to the core examination procedures, "Office of Foreign Assets Control".	
Transaction Testing	
6. On the basis of the U.S. DD's risk assessment of its foreign correspondent activities, as well as prior examination and audit reports, select a sample of higher-risk foreign correspondent financial institution account relationships. The higher-risk sample should include relationships with foreign financial institutions located in jurisdictions that do not cooperate with international AML efforts and in other jurisdictions that the U.S. DD has determined pose a higher risk. From the sample selected, perform the following examination procedures: • Review a foreign correspondent agreement or contract that delineates each party's responsibilities and the products and services provided. • Review U.S. DD statements for foreign correspondent accounts and, as necessary, specific transaction details. Compare expected transactions with actual activity. • Determine whether actual activity is consistent with the nature of the customer's business. Identify any unusual or suspicious activity. • Review large or unusual transactions to determine their nature. As necessary, obtain and review copies of credit or debit advices, general ledger tickets, and other supporting documentation. • Analyze transactions to identify behavior indicative of nested accounts,	

Procedure	Comments
intermediary or clearing agent services, or other services for third-party foreign financial institutions that have not been clearly identified.	
7. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with foreign correspondent financial institution relationships.	

4.9. Private Banking – Overview

Objective. *Assess the adequacy of the DD's systems to manage the risks associated with private banking activities, and management's ability to implement effective due diligence, monitoring, and reporting systems. This section expands the core review of the statutory and regulatory requirements of private banking in order to provide a broader assessment of the AML risks associated with this activity.*

Private banking activities are generally defined as providing personalized services to higher net worth customers (e.g., financial advice and investment management). Private banking has become an increasingly important business line for large and diverse banking organizations and a source of enhanced fee income.

For DDs, a large proportion of their customer base may be composed of high net worth and ultra-high net worth customers, including early adopters of digital assets, and family offices that are willing to undertake higher risk investment strategies, including diversification through investment in digital assets.

U.S. DDs may manage private banking relationships for both domestic and international customers. Typically, thresholds of private banking service are based on the amount of assets under management and on the need for specific products or services. The fees charged are ordinarily based on asset thresholds and the use of specific products and services.

Private banking arrangements are typically structured to have a central point of contact (i.e., relationship manager) that acts as a liaison between the client and the DD and facilitates the client's use of the DD's financial services and products. Typical products and services offered in a private banking relationship in a digital assets context include:

- Digital asset fund transfers and facilitation.
- Asset management (e.g., trust, investment advisory, investment management, and custodial and brokerage services).
- The facilitation of shell companies and offshore entities (e.g., Private Investment Companies (PIC), international business corporations (IBC), and trusts).
- Custody services and associated staking on long-term holdings.

Privacy and confidentiality are important elements of private banking relationships. Although customers may choose private banking services simply to manage their assets, they may also seek a confidential, safe, and legal haven for their capital. When acting as a fiduciary, DDs have statutory, contractual, and ethical obligations to uphold.

Risk Factors

Private banking services can be vulnerable to money laundering schemes, and past money laundering prosecutions have demonstrated that vulnerability. The 1999 Permanent Subcommittee on Investigations' Report "Private Banking and Money Laundering: A Case Study of

Opportunities and Vulnerabilities" outlined, in part, the following vulnerabilities to money laundering:

- Relationship managers as client advocates.
- Powerful clients including politically exposed persons (PEPs), industrialists, and entertainers (or other prominent individuals with outsized influence).
- Culture of confidentiality and the use of secrecy jurisdictions or shell companies.
- Private banking culture of lax internal controls.
- Competitive nature of the business.
- Significant profit potential for the service provider and relationship manager(s).

Risk Mitigation

Effective policies, procedures, and processes can help protect DDs from becoming conduits for or victims of money laundering, terrorist financing, and other financial crimes that are perpetrated through private banking relationships. Additional information relating to risk assessments and due diligence is contained in the core overview section, "Private Banking Due Diligence Program (Non-U.S. Persons)." Ultimately, illicit activities through the private banking unit could result in significant financial costs and reputational risk to the DD. Financial impacts could include regulatory sanctions and fines, litigation expenses, the loss of business, reduced liquidity, asset seizures and freezes, loan losses, and remediation expenses.

Customer Risk Assessment

DDs should assess the risks that private banking/financial services activities pose on the basis of the scope of operations and the complexity of the DD's customer relationships. Management should establish a risk profile for each customer to be used in prioritizing oversight resources and for ongoing monitoring of relationship activities. The following factors should be considered when identifying risk characteristics of private banking customers:

- **Nature of the customer's wealth and the customer's business.** The source of the customer's wealth, the nature of the customer's business, and the extent to which the customer's business history presents an increased risk for money laundering and terrorist financing. This factor should be considered for private banking accounts opened for PEPs.
- **Purpose and anticipated activity.** The size, purpose, types of accounts, products, and services involved in the relationship, and the anticipated activity of the account.
- **Relationship.** The nature and duration of the DD's relationship (including relationships with affiliates) with the private banking customer.
- **Customer's corporate structure.** Type of corporate structure (e.g., IBCs, shell companies (domestic or foreign), or PICs).
- **Geographic location and jurisdiction.** The geographic location of the private banking customer's domicile and business (domestic or foreign). The review should consider the extent to which the relevant jurisdiction is internationally recognized as presenting a

greater risk for money laundering and other higher financial crime risk activities (e.g., secrecy, tax evasion) or, conversely, is considered to have robust AML standards.

- **Public information.** Information known or reasonably available to the DD about the private banking customer. The scope and depth of this review should depend on the nature of this relationship and the risks involved.

Customer Due Diligence

CDD is essential when establishing any customer relationship and it is critical for private banking clients. DDs should take reasonable steps to establish the identity of their private banking clients and, as appropriate, the beneficial owners of accounts. Adequate due diligence should vary based on the risk factors identified previously. Policies, procedures, and processes should define acceptable CDD for different types of products (e.g., PICs), services, and accountholders. As due diligence is an ongoing process, a DD should take measures to ensure account profiles are current and monitoring should be risk-based. DDs should consider whether risk profiles should be adjusted or suspicious activity reported when the activity is inconsistent with the profile.

For purposes of the CIP, the DD is not required to search the private banking account to verify the identities of beneficiaries, but instead is only required to verify the identity of the named accountholder. However, the CIP rule also provides that, based on the DD's risk assessment of a new account opened by a customer that is not an individual (e.g., private banking accounts opened for a PIC), the DD may need "to obtain information about" individuals with authority or control over such an account, including signatories, in order to verify the customer's identity and to determine whether the account is maintained for non-U.S. persons.

Before opening accounts, DDs should collect the following information from the private banking clients:

- Purpose of the account.
- Type of products and services to be used.
- Anticipated account activity.
- Description and history of the source of the client's wealth.
- Client's estimated net worth, including financial statements.
- Current source of funds for the account.
- References or other information to confirm the reputation of the client.

Board of Directors and Senior Management Oversight

The board of directors' and senior management's active oversight of private banking activities and the creation of an appropriate corporate oversight culture are crucial elements of a sound risk management and control environment. The purpose and objectives of the organization's private banking activities should be clearly identified and communicated by the board and senior management. Well-developed goals and objectives should describe the target client base in terms of minimum net worth, investable assets, and types of products and services sought. Goals and objectives should also specifically describe the types of clients the DD will and will not accept

and should establish appropriate levels of authorization for new-client acceptance. Board and senior management should also be actively involved in establishing control and risk management goals for private banking activities, including effective audit and compliance reviews. Each DD should ensure that its policies, procedures, and processes for conducting private banking activities are evaluated and updated regularly and ensure that roles, responsibilities, and accountability are clearly delineated.

Employee compensation plans are often based on the number of new accounts established or on an increase in managed assets. Board and senior management should ensure that compensation plans do not create incentives for employees to ignore appropriate due diligence and account opening procedures, or possible suspicious activity relating to the account. Procedures that require various levels of approval for accepting new private banking accounts can minimize such opportunities.

Given the sensitive nature of private banking and the potential liability associated with it, DDs should thoroughly investigate the background of newly hired private banking relationship managers. During the course of employment, any indications of inappropriate activities should be promptly investigated by the DD.

Additionally, when private banking relationship managers change employers, their customers often move with them. DDs bear the same potential liability for the existing customers of newly hired officers as they do for any new, private banking relationship. Therefore, those accounts should be promptly reviewed using the DD's procedures for establishing new account relationships.

MIS and reports are also important in effectively supervising and managing private banking relationships and risks. Board and senior management should review relationship manager compensation reports, budget or target comparison reports, and applicable risk management reports. MIS reports should enable the relationship manager to view and manage the whole client and any related client relationships.

4.9.1. Private Banking Examination and Testing Procedures

Objective. *Assess the adequacy of the DD's systems to manage the risks associated with private banking activities, and management's ability to implement effective due diligence, monitoring, and reporting systems. This section expands the core review of the statutory and regulatory requirements of private banking in order to provide a broader assessment of the AML risks associated with this activity.*

Procedure	Comments
1. Review the policies, procedures, and processes related to private banking activities. Evaluate the adequacy of the policies, procedures, and processes given the DD's private banking activities and the risks they represent. Assess whether the controls are adequate to reasonably protect the DD from money laundering and terrorist financing.	
2. From a review of MIS reports (e.g., customer aggregation, policy exception and missing documentation, customer risk classification, unusual accounts activity, and client concentrations) and internal risk rating factors, determine whether the DD effectively identifies and monitors private banking relationships, particularly those that pose a higher risk for money laundering.	
3. Determine whether the DD's system for monitoring private banking relationships for suspicious activities, and for reporting of suspicious activities, is adequate given the DD's size, complexity, location, and types of customer relationships.	
4. Review the private banking compensation program. Determine whether it includes qualitative measures that are provided to employees to comply with account opening and suspicious activity monitoring and reporting requirements.	
5. Review the monitoring program the DD uses to oversee the private banking relationship manager's personal financial	

Procedure	Comments
condition and to detect any inappropriate activities.	
6. If appropriate, for additional guidance refer to the core examination procedures, "Office of Foreign Assets Control."	
Transaction Testing	
7. On the basis of the DD's risk assessment of its private banking activities, as well as prior examination and audit reports, select a sample of private banking accounts. The sample should include the following types of accounts: • Politically exposed persons (PEP). • Private investment companies (PIC), international business corporations (IBC), and shell companies. • Offshore entities. • Cash-intensive businesses. • Import or export companies. • Customers from or doing business in a higher-risk geographic location. • Customers listed on unusual activity monitoring reports. • Customers who have large dollar transactions and frequent funds transfers.	
8. From the sample selected, perform the following examination procedures: • Review account opening documentation and ongoing due diligence information. • Review account statements and, as necessary, specific transaction details. • Compare expected transactions with actual activity. • Determine whether actual activity is consistent with the nature of the customer's business. • Identify any unusual or suspicious activity.	

Procedure	Comments
9. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with private banking relationships.	

4.10. Non-Bank Financial Institutions – Overview

Objective. *Assess the adequacy of the DD's systems to manage the risks associated with accounts of nonbank financial institutions (NBFI), and management's ability to implement effective monitoring and reporting systems.*

NBFIs are broadly defined as institutions other than banks that offer financial services. The USA PATRIOT Act has defined a variety of entities as financial institutions. Common examples of NBFIs include, but are not limited to:

- Casinos and card clubs.
- Securities and commodities firms (e.g., brokers/dealers, investment advisers, mutual funds, hedge funds, or commodity traders).
- Money services businesses (MSB).
- Insurance companies.
- Loan or finance companies.
- Operators of credit card systems.
- Other financial institutions (e.g., dealers in precious metals, stones, or jewels; pawnbrokers).

Some NBFIs are currently required to develop an AML program, comply with the reporting and recordkeeping requirements of the BSA, and report suspicious activity, as are banks and DDs. NBFIs typically need access to banking services in order to operate. Although NBFIs maintain operating accounts at banks, the BSA does not require, and neither FinCEN nor the federal banking agencies expect, banks to serve as the *de facto* regulator of any NBFI industry or individual NBFI customer. The Department similarly does not expect DDs to serve as the *de facto* regulator of its NBFI clients. While DDs are expected to manage the risks associated with all accounts, including NBFI accounts, the Department will not hold DDs responsible for their customers' compliance with the BSA and other applicable federal and state laws and regulations.

Risk Factors

NBFI industries are extremely diverse, ranging from large multi-national corporations to small, independent businesses that offer financial services only as an ancillary component to their primary business. The range of products and services offered, and the customer bases served by NBFIs, are equally diverse. As a result of this diversity, some NBFIs may be lower risk and some may be higher risk for money laundering.

DDs that maintain account relationships with NBFIs may be exposed to a higher risk for potential money laundering activities because some NBFIs:

- Lack ongoing customer relationships and require minimal or no identification from customers.
- Maintain limited or inconsistent recordkeeping on customers and transactions.

- Engage in frequent currency transactions.
- Are subject to varying levels of regulatory requirements and oversight.
- Can quickly change their product mix or location and quickly enter or exit an operation.
- Sometimes operate without proper registration or licensing.

Risk Mitigation

DDs that maintain account relationships with NBFIs should develop policies, procedures, and processes to:

- Identify NBFI relationships.
- Assess the potential risks posed by the NBFI relationships.
- Conduct adequate and ongoing due diligence on the NBFI relationships when necessary.
- Ensure NBFI relationships are appropriately considered within the DD's suspicious activity monitoring and reporting systems.

Risk Assessment Factors

DDs should assess the risks posed by their NBFI customers and direct their resources most appropriately to those accounts that pose a more significant money laundering risk. The following factors may be used to help identify the relative risks within the NBFI portfolio. Nevertheless, management should weigh and evaluate each risk assessment factor to arrive at a risk determination for each customer and to prioritize oversight resources. Relevant risk factors include:

- Types of products and services offered by the NBFI.
- Locations and markets served by the NBFI.
- Anticipated account activity.
- Purpose of the account.
- Customer segments served by the NBFI.
- Volume of transaction activity processed by the NBFI.

A DD's due diligence should be commensurate with the level of risk of the NBFI customer identified through its risk assessment. If a DD's risk assessment indicates potential for a heightened risk of money laundering or terrorist financing, it will be expected to conduct further due diligence in a manner commensurate with the heightened risk.

Providing Financial Services to Money Services Businesses

FinCEN and the federal banking agencies issued interpretive guidance on April 26, 2005, to clarify the BSA requirements and supervisory expectations as applied to accounts opened or maintained for MSBs. With limited exceptions, many MSBs are subject to the full range of BSA regulatory requirements, including the anti-money laundering program rule, suspicious activity and currency transaction reporting rules, and various other identification and recordkeeping rules. Existing

FinCEN regulations require certain MSBs, including digital asset service providers (e.g., exchanges, ATM operators, etc.), to register with FinCEN. Finally, many states have established supervisory requirements, often including the requirement that an MSB be licensed with the state(s) in which it is incorporated or does business (money transmitter licenses).

FinCEN defines MSBs as doing business in one or more of the following capacities:

- Dealer in foreign exchange
- Check casher
- Issuer or seller of traveler's checks or money orders
- Money transmitter
- Provider of prepaid access
- Seller of prepaid access
- U.S. Postal Service

There is a threshold requirement for dealers in foreign exchange, check cashers and issuers or sellers of traveler's checks or money orders. A business that engages in such transactions will not be considered an MSB if it does not engage in such transactions in an amount greater than $1,000 for any person on any day in one or more transactions (31 CFR 1010.100(ff)). An entity that engages in money transmission in any amount is considered an MSB. In most instances, digital asset service providers/virtual currency exchangers are regulated as money transmitters. Thresholds for providers and sellers of prepaid access are discussed below.

Prepaid Access

FinCEN's regulation for MSBs excluded certain prepaid access arrangements from the definition of prepaid programs. Providers and sellers of prepaid access will not be considered an MSB if they engage in prepaid arrangements excluded from the definition of a prepaid program under 31 CFR 1010.100(ff)(4)(iii). The exclusions include arrangements that:

- Provide closed loop prepaid access to funds (i.e., such as store gift cards) in amounts not to exceed $2,000 maximum value per device on any day.
- Provide prepaid access solely to funds provided by a government agency.
- Provide prepaid access to funds for pre-tax flexible spending for health and dependent care, or from Health Reimbursement Arrangements for health care expenses.

There are two types of prepaid access arrangements that have a qualified exclusion.

- Open loop prepaid access that does not exceed $1,000 maximum value on any day.
- Prepaid access to employment benefits, incentives, wages or salaries ("payroll").

These arrangements are not prepaid programs subject to BSA regulatory requirements unless they can:

- Be used internationally.
- Allow transfers of value from person to person within the arrangement, or
- Be reloaded from a non-depository source.

If any one of these features is part of the arrangement, it will be a covered prepaid program under 31 CFR 1010.100.

Administrators and Exchangers of Virtual Currency

FinCEN's regulations define currency as "the coin and paper money of the United States or of any other country that is designated as legal tender; and that circulates; and is customarily used and accepted as a medium of exchange in the country of issuance." In contrast, "virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have legal tender status in any jurisdiction. Virtual currency must be converted into U.S. dollars through the services of an administrator or exchanger prior to deposit into the banking system. An administrator or exchanger of virtual currency is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. BSA requirements and supervisory expectations for providing banking services to administrators or exchangers of virtual currencies are the same as money transmitters.

Regulatory Expectations

The following regulatory expectations apply to DDs with MSB customers:

- The BSA does not require, and neither FinCEN nor the federal banking agencies expect, DDs to serve as the *de facto* regulator of any type of NBFI industry or individual NBFI customer, including MSBs.
- While DDs are expected to manage risk associated with all accounts, including MSB accounts, DDs will not be held responsible for the MSB's AML/CFT program.
- Not all MSBs pose the same level of risk, and not all MSBs will require the same level of due diligence. Accordingly, if a DD's assessment of the risks of a particular MSB relationship indicates a lower risk of money laundering or other illicit activity, a DD is not routinely expected to perform further due diligence (such as reviewing information about an MSB's AML/CFT program) beyond the minimum due diligence expectations. Unless indicated by the risk assessment of the MSB, DDs are not expected to routinely review an MSB's AML/CFT program.

MSB Risk Assessment

An effective risk assessment should be a composite of multiple factors, and depending upon the circumstances, certain factors may be given more weight than others. The following factors may be used to help identify the level of risk presented by each MSB customer:

- Purpose of the account.

- Anticipated account activity (type and volume).
- Types of products and services offered by the MSB.
- Locations and markets served by the MSB.

DD management may tailor these factors based on their customer base or the geographic locations in which the DD operates. Management should weigh and evaluate each risk assessment factor to arrive at a risk determination for each customer. A DD's due diligence should be commensurate with the level of risk assigned to the MSB customer, after consideration of these factors. If a DD's risk assessment indicates potential for a heightened risk of money laundering or terrorist financing, the DD will be expected to conduct further due diligence in a manner commensurate with the heightened risk.

MSB Risk Mitigation

A DD's policies, procedures, and processes should provide for sound due diligence and verification practices, adequate risk assessment of MSB accounts, and ongoing monitoring and reporting of unusual or suspicious activities. A DD that establishes and maintains accounts for MSBs should apply appropriate, specific, risk-based, and where necessary, EDD policies, procedures, and controls.

The factors below, while not all inclusive, may reduce or mitigate the risk in some MSB accounts:

- MSB is registered with FinCEN and licensed with the appropriate state(s), if required.
- MSB confirms it is subject to examination for AML compliance by the IRS or the state(s), if applicable.
- MSB affirms the existence of a written AML/CFT program and provides the BSA officer's name and contact information.
- MSB has an established banking relationship and/or account activity consistent with expectations.
- MSB is an established business with an operating history.
- MSB is a principal with one or a few agents, or is acting as an agent for one principal.
- MSB provides services only to local residents.
- Most of the MSB's customers conduct routine transactions in low dollar amounts.
- The expected (lower-risk) transaction activity for the MSB's business operations is consistent with information obtained by DD at account opening. Examples include the following:
    - Check cashing activity is limited to payroll or government checks (any dollar amount).
    - Check cashing service is not offered for third-party or out-of-state checks.
- Money-transmitting activities are limited to domestic entities (e.g., domestic bill payments) or limited to lower dollar amounts (domestic or international).

MSB Due Diligence Expectations

Registration with FinCEN, if required, and compliance with any state-based licensing requirements represent the most basic of compliance obligations for MSBs. As a result, it is reasonable and appropriate for a DD to require an MSB to provide evidence of compliance with such requirements, or to demonstrate that it is not subject to such requirements due to the nature of its financial services or status exclusively as an agent of another MSB(s).

FinCEN issued a final rule clarifying that certain foreign-located persons engaging in MSB activities within the United States fall within FinCEN's definition of an MSB and are required to register with FinCEN.

Given the importance of licensing and registration requirements, a DD should file a SAR if it becomes aware that a customer is operating in violation of the registration or state licensing requirement. There is no requirement in the BSA regulations for a DD to close an account that is the subject of a SAR. The decision to maintain or close an account should be made by DD management under standards and guidelines approved by its board of directors.

The extent to which the DD should perform further due diligence beyond the minimum due diligence obligations set forth below will be dictated by the level of risk posed by the individual MSB customer. Because not all MSBs present the same level of risk, not all MSBs will require further due diligence. For example, a local grocer that also cashes payroll checks for customers purchasing groceries may not present the same level of risk as a money transmitter specializing in cross-border funds transfers or virtual currency-related money transmission. Therefore, the customer due diligence requirements will differ based on the risk posed by each MSB customer. Based on existing BSA requirements applicable to DDs, the minimum due diligence expectations associated with opening and maintaining accounts for any MSB are:

- Apply the DD's CIP.
- Confirm FinCEN registration, if required. (Note: registration must be renewed every two years.)
- Confirm compliance with state or local licensing requirements, if applicable.
- Confirm agent status, if applicable.
- Conduct a basic AML/CFT risk assessment to determine the level of risk associated with the account and whether further due diligence is necessary.

If the DD determines that the MSB customer presents a higher level of money laundering or terrorist financing risk, EDD measures should be conducted in addition to the minimum due diligence procedures. Depending on the level of perceived risk, and the size and sophistication of the particular MSB, banking organizations may pursue some or all of the following actions as part of an appropriate EDD review:

- Review the MSB's AML/CFT program.
- Review results of the MSB's independent testing of its AML program.
- Review written procedures for the operation of the MSB.
- Conduct on-site visits.

- Review list of agents, including locations, within or outside the United States, which will be receiving services directly or indirectly through the MSB account.
- Determine whether the MSB has performed due diligence on any third-party servicers or paying agents.
- Review written agent management and termination practices for the MSB.
- Review written employee screening practices for the MSB.
- Where the NBFI is a virtual currency money transmitter.

FinCEN and the federal banking agencies do not expect DDs to uniformly require any or all of the actions identified above for all MSBs.

4.10.1. Nonbank Financial Institutions Examination and Testing Procedures

Objective. *Assess the adequacy of the DD's systems to manage the risks associated with accounts of nonbank financial institutions (NBFI), and management's ability to implement effective monitoring and reporting systems.*

Procedure	Comments
1. Determine the extent of the DD's relationships with NBFIs and, for DDs with significant relationships with NBFIs, including digital asset service providers/virtual currency exchangers, review the DD's risk assessment of this activity.	
2. Review the policies, procedures, and processes related to NBFI accounts. Evaluate the adequacy of the policies, procedures, and processes given the DD's NBFI activities and the risks they represent. Assess whether the controls are adequate to reasonably protect the DD from money laundering and terrorist financing.	
3. From review of MIS and internal risk rating factors, determine whether the DD effectively identifies and monitors NBFI accounts.	
4. Determine whether the DD's system for monitoring NBFI accounts for suspicious activities, and for reporting of suspicious activities, is adequate given the nature of the DD's customer relationships.	
Money Services Businesses	
5. Consistent with the interagency guidance released on April 26, 2005, determine whether the DD has policies, procedures, and processes for accounts opened or maintained for money services businesses (MSB) to: • Apply the DD's CIP	

Procedure	Comments
• Confirm FinCEN registration, if required. (Note: registration must be renewed every two years.) • Confirm state licensing, if applicable. • Confirm agent status, if applicable. • Conduct a risk assessment to determine the level of risk associated with each account and whether further due diligence is required.	
6. Determine whether the DD's policies, procedures, and processes to assess risks posed by MSB customers effectively identify higher risk accounts and the amount of further due diligence necessary.	
Transaction Testing	
7. On a basis of the DD's risk assessment of its NBFI accounts, as well as prior examination and audit reports, select a sample of higher-risk NBFI accounts. From the sample selected, perform the following examination procedures: • Review account opening documentation and ongoing due diligence information. • Review account statements and, as necessary, specific transaction details. Compare expected transactions with actual activity. • Determine whether actual activity is consistent with the nature of the customer's business and identify any unusual or suspicious activity.	
8. On a basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with NBFI relationships.	

4.11. Business Entities (Domestic and Foreign) – Overview

Objective. *Assess the adequacy of the DD's systems to manage the risks associated with transactions involving domestic and foreign business entities, and management's ability to implement effective due diligence, monitoring, and reporting systems.*

The term "business entities" refers to limited liability companies, corporations, trusts, and other entities that may be used for many purposes. Business entities are relatively easy to establish. Individuals, partnerships, and existing corporations establish business entities for legitimate reasons, but the entities may be abused for money laundering and terrorist financing.

Domestic Business Entities

All states have statutes governing the organization and operation of business entities, including limited liability companies, corporations, general partnerships, limited partnerships, and trusts. Shell companies registered in the United States are a type of domestic business entity that may pose heightened risks. Shell companies can be used for money laundering and other crimes because they are easy and inexpensive to form and operate. In addition, ownership and transactional information can be concealed from regulatory agencies and law enforcement, in large part because most state laws require minimal disclosures of such information during the formation process. According to a report by the U.S. Government Accountability Office (GAO), law enforcement officials are concerned that criminals are increasingly using U.S. shell companies to conceal their identity and illicit activities.

Shell companies can be publicly traded or privately held. Although publicly traded shell companies can be used for illicit purposes, the vulnerability of the shell company is compounded when it is privately held and beneficial ownership can more easily be obscured or hidden. Lack of transparency of beneficial ownership can be a desirable characteristic for some legitimate uses of shell companies, but it is also a serious vulnerability that can make some shell companies ideal vehicles for money laundering and other illicit financial activity. In some state jurisdictions, only minimal information is required to register articles of incorporation or to establish and maintain "good standing" for business entities — increasing the potential for their abuse by criminal and terrorist organizations.

Foreign Business Entities

Frequently used foreign entities include trusts, investment funds, and insurance companies. Two foreign entities that can pose particular money laundering risk are international business corporations (IBC) and Private Investment Companies (PIC) opened in offshore financial centers (OFC). Many OFCs have limited organizational disclosure and recordkeeping requirements for establishing foreign business entities, creating an opportune environment for money laundering.

International Business Corporations

IBCs are entities formed outside of a person's country of residence which can be used to maintain confidentially or hide assets. IBC ownership can, based on jurisdiction, be conveyed through registered or bearer shares. There are a variety of advantages to using an IBC which include, but are not limited to, the following:

- Asset protection.
- Estate planning.
- Privacy and confidentiality.
- Reduction of tax liability.

Through an IBC, an individual is able to conduct the following:

- Open and hold DD accounts.
- Hold and transfer funds.
- Engage in international business and other related transactions.
- Hold and manage offshore investments (e.g., stocks, bonds, mutual funds, and certificates of deposit), many of which may not be available to "individuals" depending on their location of residence.

Private Investment Companies

PICs are separate legal entities. They are essentially subsets of IBCs. Determining whether a foreign corporation is a PIC is based on identifying the purpose and use of the legal vehicle. PICs are typically used to hold individual funds and investments, and ownership can be vested through bearer shares or registered shares. Like other IBCs, PICs can offer confidentiality of ownership, hold assets centrally, and may provide intermediaries between private banking customers and the potential beneficiaries of the PICs. Shares of a PIC may be held by a trust, which further obscures beneficial ownership of the underlying assets. IBCs, including PICs, are frequently incorporated in countries that impose low or no taxes on company assets and operations or are DD secrecy havens.

Decentralized Autonomous Organizations ("DAOs")

DAOs are organizations or businesses that leverage the blockchain's smart contract technology[351] to make shared decisions on behalf of its members, with every vote or action that takes place being

[351] "A smart contact is an automated transaction, as defined in W.S. 40-21-102(a)(ii), or any substantially similar analogue, which is comprised of code, script or programming language that executes the terms of an agreement and which may include taking custody of and transferring an asset, administrating membership interest votes with respect to a decentralized autonomous organization or issuing executable instructions for these actions, based on the occurrence or nonoccurrence of specified conditions." Wyoming Secretary of State Business Division, "Decentralized Autonomous Organization (DAO): Frequently Asked Questions" (March 2022).

represented in the form of a transaction on the blockchain.[352] In 2021, Wyoming became the first state to pass legislation into law recognizing DAOs and allowing DAOs to register as distinct limited liability companies ("LLCs") in the state of Wyoming, thereby being the first official regulator of DAOs when the law became effective on July 1, 2021.[353] As the sole state regulator of DAOs, Wyoming has a series of requirements that DAOs must follow if they want to be recognized LLCs domiciled in Wyoming. For example:

- Name has to include "LLC" and "DAO" or "LAO;" and
- Articles of Organization have to include a publicly available identifier of any smart contract directly used to facilitate, manage or operate the DAO, among other pieces of information).[354]

In the event that a DD seeks to onboard a DAO, it must pay particular attention to the nature and purpose of the DAO and its source of funds, given that activity associated with fundraising is likely to entail higher ML/TF and sanctions risk than other activities in which a DAO can engage, such as general voting, governance, and participation in a social network. DAOs that offer and sell securities in the U.S. must also comply with applicable SEC federal securities laws.[355]

Nominee Incorporation Services

Intermediaries, called nominee incorporation services (NIS), establish U.S. shell companies and DD accounts on behalf of foreign clients. NIS may be located in the United States or offshore. Corporate lawyers in the United States often use NIS to organize companies on behalf of their domestic and foreign clients because such services can efficiently organize legal entities in any state. NIS must comply with applicable state and federal procedures as well as any specific DD requirements. Those laws and procedures dictate what information NIS must share about the owners of a legal entity. Money launderers have also utilized NIS to hide their identities. By hiring a firm to serve as an intermediary between themselves, the licensing jurisdiction, and the DD, a company's beneficial owners may avoid disclosing their identities in state corporate filings and in corporate DD account opening documentation.

An NIS has the capability to form business entities, open full-service DD accounts for those entities, and act as the registered agent to accept service of legal process on behalf of those entities in a jurisdiction in which the entities have no physical presence. Furthermore, an NIS can perform

---

[352] IncParadise, "Decentralized Autonomous Organization (DAO) in Wyoming" (2022).

[353] State of Wyoming Legislature, "SF0038 - Decentralized autonomous organizations" (2021).

[354] IncParadise, "Decentralized Autonomous Organization (DAO) in Wyoming" (2022).

[355] Westlaw Today, "Wyoming Passes DAO Supplement Recognizing Decentralized Autonomous Organizations (DAOs) as LLCs" (September 2021).

these services without ever having to identify beneficial ownership on company formation, registration, or DD account documents.

Several international NIS firms have formed partnerships or marketing alliances with U.S. DDs to offer financial services such as Internet banking and funds transfer capabilities to shell companies and non-U.S. citizens. U.S. DDs participating in these marketing alliances by opening accounts through intermediaries without requiring the actual accountholder's physical presence, accepting by mail copies of passport photos, utility bills, and other identifying information may be assuming increased levels of AML/CFT risk.

Risk Factors

Money laundering and terrorist financing risks arise because business entities can hide the true owner of assets or property derived from or associated with criminal activity. The privacy and confidentiality surrounding some business entities may be exploited by criminals, money launderers, and terrorists. While the form that business entities and legal arrangements can take is varied, a common feature of most models is a general lack of transparency, which challenges AML/CFT and sanctions compliance efforts.

Verifying the grantors and beneficial owner(s) of some business entities may be extremely difficult, as the characteristics of these entities shield the legal identity of the owner. Few public records will disclose true ownership. Overall, the lack of ownership transparency; minimal or no recordkeeping requirements, financial disclosures, and supervision; and the range of permissible activities all increase money laundering risk, and in some cases raise sanctions exposure risks, particularly where such exposure may be associated with oligarchs and other high net worth SDNs.

While business entities can be established in most international jurisdictions, many are incorporated in OFCs that provide ownership privacy and impose few or no tax obligations. To maintain anonymity, many business entities are formed with nominee directors, officeholders, and shareholders. In certain jurisdictions, business entities can also be established using bearer shares; ownership records are not maintained, rather ownership is based on physical possession of the stock certificates. Revocable trusts are another method used to insulate the grantor and beneficial owner and can be designed to own and manage the business entity, presenting significant barriers to law enforcement.

Shell Companies

Shell companies also pose significant ML/TF and sanctions risk. While the majority of U.S.-based shell companies serve legitimate purposes, some shell companies have been used as conduits for money laundering, to hide overseas transactions, or to layer domestic or foreign business entity structures. For example, regulators have identified shell companies registered in the United States conducting suspicious transactions with foreign-based counterparties. These transactions, primarily funds transfers circling in and out of the U.S. banking system, evidenced no apparent

business purpose. Domestic business entities with bank-like names, but without regulatory authority to conduct banking, should be particularly suspect.

The following indicators of potentially suspicious activity may be commonly associated with shell company activity:

- Insufficient or no information available to positively identify originators or beneficiaries of funds transfers (using Internet, commercial database searches, or direct inquiries to a respondent bank).
- Payments have no stated purpose, do not reference goods or services, or identify only a contract or invoice number.
- Goods or services, if identified, do not match profile of company provided by respondent bank or character of the financial activity; a company references remarkably dissimilar goods and services in related funds transfers; explanation given by foreign respondent bank is inconsistent with observed funds transfer activity.
- Transacting businesses share the same address, provide only a registered agent's address, or other address inconsistencies.
- Many or all of the funds transfers are sent in large, round dollar, hundred dollar, or thousand dollar amounts. Unusually large number and variety of beneficiaries receiving funds transfers from one company.
- Frequent involvement of multiple jurisdictions or beneficiaries located in higher-risk OFCs.
- A foreign correspondent bank exceeds the expected volume in its client profile for funds transfers, or an individual company exhibits a high volume and pattern/amount of funds transfers/sporadic activity that is inconsistent with its normal business activity/patterns.
- Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.
- Purpose of the shell company is unknown or unclear.

Decentralized Autonomous Organizations

DAOs, due to their novel structure, nascent regulatory framework, and generally pseudonymous nature tend to pose unique AML/CFT and sanctions compliance challenges. There are several KYC challenges associated with DAOs and decentralized entities, more generally.[356] Specifically, the participants in a DAO typically participate through pseudonymous public addresses and the identity of DAO participants, including key decision-makers, is not known. Further, unlike in the case of typical legal entities and legal arrangements where there exist beneficial owners and controllers, in the case of DAOs, while members of a DAO operate with a shared purpose, they typically do not have a central controller who directs the group. Decisions are made collectively in a decentralized fashion by consensus, with the parties to the DAO rarely, if ever, interacting with one another in-person, and often not even knowing the legal names and identities of DAO

[356] Financial Times "Cryptocurrency: rise of decentralised finance sparks 'dirty money' fears" (September 2021).

member participants. Moreover, DAOs themselves are at risk of being exploited by illicit actors, such as in the case of smart contract code vulnerabilities. There have been several hacks of DAOs leading to the theft of millions of dollars in cryptocurrency by illicit actors who then proceeded to launder the funds.[357]

Risk Mitigation

Management should develop policies, procedures, and processes that enable the DD to identify account relationships, in particular deposit accounts, with business entities, and monitor the risks associated with these accounts in all the DD's departments. Management should establish appropriate due diligence at account opening and during the life of the relationship to manage risk in these accounts. In the case of DAOs, management may be required to monitor evolving industry practices and align internal controls accordingly to match new developments and controls.

The DD should gather sufficient information on the business entities and their beneficial owners to understand and assess the risks of the account relationship. Important information for determining the valid use of these entities includes the type of business, the purpose of the account, the source of funds, and the source of wealth of the owner or beneficial owner.

The DD's CIP should detail the identification requirements for opening an account for a business entity. When opening an account for a customer that is not an individual, DDs are permitted by 31 CFR 1020.100 to obtain information about the individuals who have authority and control over such accounts in order to verify the customer's identity (the customer being the business entity). Required account opening information may include articles of incorporation, a corporate resolution by the directors authorizing the opening of the account, or the appointment of a person to act as a signatory for the entity on the account. Particular attention should be paid to articles of association that allow for nominee shareholders, board members, and bearer shares.

If the DD is facilitating the establishment of a business entity for a new or existing customer, the money laundering risk to the DD is typically mitigated. Because the DD is aware of the parties (e.g., grantors, beneficiaries, and shareholders) involved in the business entity, initial due diligence and verification is easier to obtain. Furthermore, in such cases, the DD frequently has ongoing relationships with the customers initiating the establishment of a business entity.

Risk assessments may include a review of the domestic or international jurisdiction where the business entity was established, the type of account (or accounts) and expected versus actual transaction activities, the types of products that will be used, and whether the business entity was created in-house or externally. If ownership is held in bearer share form, DDs should assess the risks these relationships pose and determine the appropriate controls. For example, in most cases DDs should choose to maintain (or have an independent third party maintain) bearer shares for

[357] JD Supra, "Crypto, DAOs, and the Wyoming Frontier" (July 2021).

customers. In rare cases involving lower-risk, well-known, established customers, DDs may find that periodically recertifying beneficial ownership is effective. The DD's risk assessment of a business entity customer becomes more important in complex corporate formations. For example, a foreign IBC may establish a layered series of business entities, with each entity naming its parent as its beneficiary.

Ongoing account monitoring is critical to ensure that the accounts are reviewed for unusual and suspicious activity. The DD should be aware of higher-risk transactions in these accounts, such as activity that has no business or apparent lawful purpose, funds transfer activity to and from higher-risk jurisdictions, currency intensive transactions, and frequent changes in the ownership or control of the nonpublic business entity.

When onboarding and performing due diligence on novel business entities/legal arrangements, such as DAOs, DDs may consider adopting specialized due diligence requirements. Such requirements may include, but need not be limited to the following:

- Assessing the legal status of the DAO and any information available about its members;
- Assessing the nature and purpose of the DAO, including its mission, its founders (where applicable), and whether the DAO has an explicit-time bound goal;
    - Where the purpose of the DAO is to engage in fundraising activity, determine the purpose of the fund raising and what, if any, risk mitigation measures are placed around received deposits;
- Assessing the DAO’s purpose for establishing an account with the DD;
    - Where the purpose of the account is depositing funds on behalf of the DAO, assessing the source of funds, including performing provenance analysis/transaction tracing on the source of the funds.

4.11.1. Business Entities (Domestic and Foreign) Examination and Testing Procedures

Objective. *Assess the adequacy of the DD's systems to manage the risks associated with transactions involving domestic and foreign business entities, and management's ability to implement effective due diligence, monitoring, and reporting systems.*

Procedure	Comments
1. Review the DD's policies, procedures, and processes related to business entities. Evaluate the adequacy of the policies, procedures, and processes given the DD's transactions with business entities and the risks they present. Assess whether the controls are adequate to reasonably protect the DD from money laundering and terrorist financing.	
2. Review the policies and processes for opening and monitoring accounts with business entities. Determine whether the policies adequately assess the risk between different account types.	
3. Determine how the DD identifies and, as necessary, completes additional due diligence on business entities (including beneficial ownership identification and verification). Assess the level of due diligence the DD performs when conducting its risk assessment.	
4. From a review of MIS and internal risk rating factors, determine whether the DD effectively identifies and monitors higher-risk business entity accounts.	
5. Determine whether the DD's system for monitoring business entities for suspicious activities, and for reporting of suspicious activities, is adequate given the activities associated with business entities.	
6. If appropriate, for additional guidance refer to the core examination procedures, "Office of Foreign Assets Control."	

Procedure	Comments
Transaction Testing	
7. On the basis of the DD's risk assessment of its accounts with business entities, as well as prior examination and audit reports, select a sample of these accounts. Include the following risk factors: • An entity organized in a higher-risk jurisdiction. • Account activity that is substantially currency based. • An entity whose account activity consists primarily of circular-patterned funds transfers. • A business entity whose ownership is in bearer shares, especially those whose bearer shares are not under DD or trusted third-party control. • An entity that uses a wide range of DD services, particularly trust and correspondent services. • An entity whose business model is particularly novel and subject to nascent regulatory requirements (e.g., DAO). • An entity owned or controlled by other nonpublic business entities. • Business entities for which the DD has filed SARs.	
8. From the sample selected, obtain a relationship report for each selected account. It is critical that the full relationship, rather than only an individual account, be reviewed.	
9. Review the due diligence information on the business entity. Assess the adequacy of that information.	
10. Review account statements and, as necessary, specific transaction details. Compare expected transactions with actual activity. Determine whether actual activity	

Procedure	Comments
is consistent with the nature and stated purpose of the account and whether transactions appear unusual or suspicious. Areas that may pose a higher risk, such as funds transfers, private banking, trust, and monetary instruments, should be a primary focus of the transaction review.	
11. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with business entity relationships.	

V. APPENDIX

Appendix A: List of Digital Assets Guidance and Supervision from Other Jurisdictions

A number of supervisory bodies have developed regulations, supervisory guidance, and other descriptions of digital assets, including virtual currency, that address money laundering, terrorist financing, sanctions evasion, and other illicit activity. Recognizing that supervision of digital assets is an evolving space, the Department highlights a select set of domestic and international jurisdictional guidance—both regulatory and industry guidance—as additional reference points for supervisory and control framework considerations.

Note that this appendix includes an "as of date" of June 2022, and will be updated with each DD AML & OFAC Manual update.

Source	Reference Material
Applicable U.S. federal and state standards for reference	• Department of Justice: Attorney General's Cyber-Digital Task Force: DOJ (October 2020) released "Cryptocurrency: An Enforcement Framework" • Federal Reserve SR 11-7: Guidance on Model Risk Management (April 4, 2011) • FFIEC AML Manual: April 2020 update • FFIEC AML Manual: 2021 updates • FinCEN: *Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets* (January 2021) • FinCEN: Frequently Asked Questions Regarding Requirements for Certain Transactions Involving Certain CVC or Digital Assets (June 2021) • FinCEN, "FinCEN Provides Financial Institutions with Red Flags on Potential Russian Sanctions Evasion Attempts" (March 7, 2022) • FinCEN: Frequently Asked Questions Regarding Customer Due Diligence (CDD) Requirements for Covered Financial Institutions (August 3, 2020) • FinCEN: *Advisory on Illicit Activity Involving Convertible Virtual Currency* (May 9, 2019) • FinCEN's May 9, 2019: *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*

- FinCEN's March 18, 2013: *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*
- FinCEN's June 2021: *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities*
- FinCEN's November 2021: *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*
- FinCEN's March 2022: *FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts*
- FDIC, "Financial Institution Letter: Notification of Engaging in Crypto-Related Activities (FIL-16-2022)" (April 2022).
- Government Accountability Office, "Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking" (December 2021).
- Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, "Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance" (April 2021)
- President's Working Group on Financial Markets, FDIC, and OCC, "Report on Stablecoins" (November 2021).
- New York Department of Financial Services Part 200 (Virtual Currencies) including 200.15 (Anti-Money Laundering Program) and (Proposed Guidance Regarding Adoption or Listing of Virtual Currencies)
- NYDFS Part 504 (Banking Department Transaction Monitoring and Filtering Program Requirements and Certifications)
- NYDFS: *Guidance on Use of Blockchain Analytics* (April 28, 2022)
- U.S. Treasury's March 2022: *National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing*
- White House: *United States Strategy on Countering Corruption* (December 2021)
- White House: *Executive Order on Ensuring Responsible Development of Digital Assets* (March 2022)
- Office of the Comptroller of the Currency: *OCC Issues Consent Order Against Anchorage Digital Bank* (April 21, 2022)
- OFAC's September 2021: *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*

	• OFAC's October 2021: *Sanctions Compliance Guidance for Virtual Currency Industry* • OFAC (A Framework for OFAC Compliance Commitments)
Select Foreign- standards	• Abu Dhabi Financial Services Regulatory Authority jurisdiction (Guidance – Regulation of Virtual Asset Activities in ADGM) • Bermuda Monetary Authority (Sector-Specific Guidance Notes for Digital Asset Business (DAB)) • Central Bank of Bahrain (Anti-Money Laundering and Combating of Financial Crime Module [Volume 6: Capital Markets]) • European Union (5th AML Directive or ("5MLD") • European Union: *Proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets* (July 2021) • EU Parliament, "EU Parliament Votes to Impose KYC on Private Crypto Wallets" (March 2022) • Korea Financial Intelligence Unit (Anti-Money Laundering Guidelines on Virtual Currency) • Monetary Authority of Singapore (Payment Service Act 2019) (New regulatory framework to enhance payment services in Singapore) (Guidelines to MAS Notice PS-N02 On Prevention of Money Laundering and Countering the Financing of Terrorism) • Swiss Financial Market Supervisory Authority (Guidance 02/2019 Payment on the Blockchain)(Legal framework for distributed ledger technology and blockchain in Switzerland) • United Kingdom Financial Conduct Authority and Joint Money Laundering Steering Group (Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3 as well as Cryptoasset exchange providers and custodian wallet providers)
Industry Guidance:	• Asia Securities Industry and Financial Markets Association (Best Practices for Digital Asset Exchanges) • Elliptic (November 2021), "Crypto Addresses Holding NFTs Worth $532k are Among the Latest Sanctioned by OFAC" • FATF (Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers) • FATF (2020), 12 Month Review of Revised FATF Standards - Virtual Assets and VASPs. • FATF, "Guidance on Digital Identity" (March 2020). • FATF (2021), Second 12 Month Review of Revised FATF Standards - Virtual Assets and VASPs

- Global Digital Finance (Principles for KYC / AML)
- Treasury, "Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art", (February 2022).
- Certified Financial Crime Specialists "Privacy Wallets and Crypto Crime – A Top Trend in Illicit Use of Cryptocurrencies" (February 2021).
- Elliptic "Over 13% of all Proceeds of Crime in Bitcoin are Now Laundered Through Privacy Wallets" (December 2020).
- Wyoming Secretary of State Business Division, "DAO Frequently Asked Questions" (March 2022).
- State of Wyoming Legislature, "SF0038 - Decentralized autonomous organizations" (2021).
- IncParadise, "Decentralized Autonomous Organization (DAO) in Wyoming" (2022).
- Westlaw Today, "Wyoming Passes DAO Supplement Recognizing Decentralized Autonomous Organizations (DAOs) as LLCs" (September 2021).
- JD Supra, "Crypto, DAOs, and the Wyoming Frontier" (July 2021).
- Financial Times "Cryptocurrency: rise of decentralised finance sparks 'dirty money' fears" (September 2021).

Appendix B: Money Laundering and Terrorist Financing Red Flags Associated with Digital Assets

The following are examples of risk typologies and 'red flags' currently identified within the digital asset space based on industry and regulatory guidance. The sections below include 'red flags' identified by FinCEN in its *Advisory on Illicit Activity Involving Convertible Virtual Currency*, which provides specific typologies that FinCEN and other law enforcement agencies have observed. The document also considers typologies identified by the industry including industry working groups, blockchain analytics providers, and industry white papers.[358]

The typologies within this section are not comprehensive and will continue to develop as the digital asset space matures. DDs should remain observant for emerging risk typologies beyond those included in this section on an ongoing basis, including those identified in *Appendix F. Money Laundering and Terrorist Financing Red Flags* of the FFIEC AML Manual to determine whether illicit activity commonly associated with other similar fiat-based instruments (e.g., use of cash or precious metals) is also applicable to the DD's business model.

In addition, DDs should consider FATF's September 2020 "FATF Report – Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing," which provides a number of virtual currency-specific red flags, including related to transactions, transaction patterns, anonymity, senders or recipients, sources of funds or wealth, and geographical risks.[359]

DDs and examiners may find this list helpful in identifying circumstances that warrant additional scrutiny. Those typologies highly correlated to illicit activity (e.g., darknet marketplaces) should be investigated even when observed without additional suspicious indicators, though the mere presence of some other typologies does not necessarily indicate the presence of criminal activity. As in traditional financial services, management's primary focus should be on reporting suspicious activities, rather than on determining whether the transactions are in fact linked to money laundering, terrorist financing, or a particular crime.[360] For more information regarding SAR reporting in the digital asset space, refer to "*3.3. Suspicious Activity Reporting*" section of this document.

---

[358] Banks may also consider typologies as presented by Project Participate, which describes itself as an "informal industry-led working group that aims to bolster the capabilities of VASPs to identify and report suspicious activity by convening industry participants to share, discuss and publish indicators of suspicion for potential crimes related to virtual assets."

[359] FATF, *FATF Report – Red Flag Indicators of Money Laundering and Terrorist Financing* (September 2020).

[360] "Management's primary focus should be on reporting suspicious activities, rather than on determining whether the transactions are in fact linked to money laundering, terrorist financing, or a particular crime." See opening paragraph of FinCEN's "Appendix F: Money Laundering and Terrorist Financing Red Flags" (June 2020).

The key risks discussed in this appendix include:

- Darknet marketplaces,
- Peer to peer (P2P) exchanges;
- Unregistered and foreign-located money service providers (MSBs);
- CVC kiosks (or "crypto ATMs");
- Attempted concealing of identity and source of funds (including the use of mixers and tumblers);
- Privacy coins without a legitimate use, especially when a customer refuses to provide identifying information or transaction data to facilitate appropriate screening, as well as other AECs;
- Privacy wallets;
- Online gambling and gaming (including virtual currency casinos); and
- Decentralized exchanges.

Darknet Marketplaces

Darknet marketplaces are websites that are only available in anonymized overlay networks that require specific software to access. An overlay network is a telecommunications network that is built on top of another network and is supported by its infrastructure.[361]

These marketplaces are known to include illicit activity from drug sales to child exploitation, often with digital assets as the primary or sole form of payment. As such, a customer or digital asset with a history of darknet marketplace activity indicates a high risk for criminal activity, and warrants investigation. Further, many of the money service businesses ("MSBs") facilitating transactions on darknet marketplaces have not registered with FinCEN and are therefore operating illegally.

Users can engage with dark marketplaces directly as a provider or administrator, as well as indirectly as a transaction participant. A user is more likely to be a darknet service provider if they transact frequently with multiple third parties, in a manner similar to a typical retail operation. Indirect connections to darknet marketplaces may be observed through the movement of digital assets from a user's wallet to a darknet wallet within a short time frame and in a similar amount.

FinCEN has provided a series of flags that indicate elevated risk of illicit activity through darknet marketplaces, including:

- A customer conducts transactions with CVC addresses that have been linked to darknet marketplaces or other illicit activity.

[361] Definition provided on page three (3) of FinCEN's "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 2019).

- A customer's CVC address appears on public forums associated with illegal activity.
- A customer's transactions are initiated from IP addresses associated with Tor.
- Blockchain analytics indicate that the wallet transferring CVC to the exchange has a suspicious source or sources of funds, such as a darknet marketplace.
- A transaction makes use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces.[362]

Industry guidance has identified additional darknet marketplace-related indicators, including:

- A customer is found to have been connected to Tor through the user's IP address or Internet Service Provider ("ISP").
- Funds moved from the darknet wallet to a customer's wallet in a short time frame.
- A customer utilizes anonymizing services such as VPN networks, privacy coins, and mixer/tumblers in the absence of other justifications like IT security or privacy and the customer provides additional data.
- A customer frequently receives funds from, or sends funds to, darknet wallet addresses that accumulate to large values.
- A significant percentage of a customer's deposits to an exchange originate from darknet marketplaces.
- A significant percentage of a customer's withdrawals from an exchange ultimately result in transactions with darknet marketplaces.[363]

Unregistered Peer-to-Peer ("P2P") Exchangers

P2P exchangers are individuals or entities offering to exchange fiat currencies for virtual currencies or one virtual currency for another virtual currency.[364] These exchanges allow users to choose specific counterparties to trade with, often without a formal KYC or CDD process. P2P exchanges should be distinguished from order-based exchanges that arrange trades by matching different user bids based on price and order size.

FinCEN has clarified that such exchangers function as MSBs and are therefore subject to registration and relevant BSA compliance. Most P2P exchangers, however, fail to register with FinCEN, and therefore may not implement controls needed to mitigate facilitating criminal

[362] See "Red Flag Indicators of the Abuse of Virtual Currencies" section of FinCEN's "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 2019).

[363] See Sections 6.6 and 6.7 from "Indicators of Suspicion for Virtual Asset Service Providers" (2019).

[364] Definition provided on page four (4) of FinCEN's "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 19, 2019).

activity.[365] Certain P2P exchangers attempt to avoid recognition by deliberately misrepresenting or obfuscating their activity, often through the use of money mules[366] and mixers in the absence of legitimate uses for mixers or tumblers, including IT security or privacy.[367] The limited or absent KYC taking place at these exchanges, as well as their known links to money laundering, require that DDs monitor for direct and indirect links to such exchangers.

FinCEN has provided a series of flag that indicate elevated risk of illicit activity through P2P exchanges, including:

- A customer receives multiple cash deposits or wires from disparate jurisdictions, branches of a financial institution, or persons and shortly thereafter uses such funds to acquire virtual currency.
- A customer receives a series of deposits from disparate sources that, in aggregate, amount to nearly identical aggregate funds transfers to a known virtual currency exchange platform within a short period of time.
- A customer's phone number or email address is connected to a CVC P2P exchange platform advertising exchange services.[368]

Industry guidance has identified additional P2P-related indicators, including:

- Funds are deposited soon after account registration and withdrawn again shortly thereafter in the same virtual asset without using platform features (e.g., trading/margin funding).
- Funds are primarily sent to or received from P2P exchanges without using the platform's features, particularly fiat transactions.
- A customer has a high frequency of deposits or withdrawals with unknown third parties.
- Amount of funding is not consistent with the customer's net worth or declared income.
- A large amount (i.e., hundreds) of deposits and/or withdrawals to different individual wallet clusters, where only one transaction is sent to each wallet cluster. This may be indicative that the user is exchanging fiat for virtual assets in person.

---

[365] Department of Justice: Attorney General's Cyber-Digital Task Force, "DOJ released 'Cryptocurrency: An Enforcement Framework'" (October 2020).

[366] Money mules refer to third parties used to carry out transactions on behalf of another individual. See "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 2019).

[367] Mixing or tumbling involves the use of mechanisms to break the connection between an address sending CVCs and the addresses receiving CVCs. See "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 2019).

[368] See "Red Flag Indicators of the Abuse of Virtual Currencies" section of FinCEN's "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 2019).

- A customer's trading activity does not correlate logically with day-to-day movements in the price of digital assets.[369,370]

Unregistered Foreign-Located MSBs

Unregistered foreign-located MSBs describe digital asset exchanges that operate in jurisdictions without clear KYC/CFT requirements and do not comply with the KYC/CFT established by the United States.[371] FinCEN has clarified that a foreign-located business qualifies as an MSB if it does business as an MSB wholly or in substantial part within the United States (31 CFR § 1010.100(ff)).

Similar to P2P exchanges, unregistered foreign-located MSBs allow parties to transact in digital assets with additional anonymity. Unlike P2P exchanges, unregistered foreign-located MSBs often appear legitimate as they can produce corporate documentation and may appear to operate as a registered exchange.

FinCEN has provided a series of indicators that indicate elevated risk of illicit activity through unregistered foreign-located MSBs, including:

- A customer transfers or receives funds, including through traditional banking systems, to or from an unregistered foreign CVC exchange or other MSB with no relation to where the customer lives or conducts business.
- A customer utilizes a CVC exchanger or foreign-located MSB in a high-risk jurisdiction lacking, or known to have inadequate AML/CFT regulations for CVC entities, including inadequate KYC or customer due diligence measures.
- A customer directs large numbers of CVC transactions to CVC entities in jurisdictions with reputations for being tax havens.
- A customer that has not identified itself to the exchange, or registered with FinCEN, as a money transmitter appears to be using the liquidity provided by the exchange to execute large numbers of offsetting transactions, which may indicate that the customer is acting as an unregistered MSB.[372]

---

[369] See Sections 6.9 and 6.11 from "Indicators of Suspicion for Virtual Asset Service Providers" (2019).

[370] See Part 3 of Elliptic's "Money Laundering & Terrorist Financing Typologies in Cryptocurrencies" (March 2020).

[371] Definition provided on page 6 of FinCEN's "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 2019).

[372] See "Red Flag Indicators of the Abuse of Virtual Currencies" section of FinCEN's "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 2019).

Industry guidance has identified additional unregistered MSB-related indicators focused on the identification of such MSBs, including:

- A customer is unable to provide confirmation that it is registered with a financial authority, when it should be so registered based on geographic location.
- A customer advises that the regulations for its jurisdiction are obscure or do not require registration with a financial authority.
- A customer's AML/KYC policy and procedures have been copied and pasted from a public source with minimal or no customization for the user's inherent risk.
- A customer takes an inordinate amount of time to produce AML/KYC policy and procedures and compliance officer information.
- A customer conducting transactions appears to be inconsistent with user's KYC (may occur if onboarded under false pretenses, or where the customer's actual activity is inconsistent with stated intended activity).
- A large amount (i.e., hundreds) of deposits and/or withdrawals to different individual wallet clusters, where only one transaction is sent to each wallet cluster. This may be indicative that the user is exchanging fiat for virtual assets in person, which may be illegal in some countries.
- A customer has a history with an exchange that warns customers not to make mention of digital assets when communicating with external parties such as DDs. Or, customers are instructed by the exchange to put vague or misleading information into wire transfer message fields when transferring fiat funds to or from a DD.
- A customer has a history with an exchange that permits customers to fund their account even if they have received virtual currency directly from mixers/tumblers and the DD cannot establish with reasonable certainty that the customer did not have a reasonable IT security or privacy concern.
- A customer has a history with an exchange that may have registered only recently and may have no prior established history of virtual currency trading.
- A customer has a history with an exchange that is associated with open discussions among criminals on the dark web.

CVC Kiosks

CVC Kiosks (a.k.a., crypto-ATMs) are ATM-like devices or electronic terminals that allow users to exchange cash and digital assets.[373] These services present heightened risk as the source of fiat funds used in these kiosks are nearly untraceable without necessary AML/KYC processes.

[373] Definition provided on page 7 of FinCEN's "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 2019).

FinCEN has noted that many kiosks not only lack such KYC processes but "have operated in ways that suggest a willful effort to evade BSA requirements." In guidance published in October 2020, the DOJ stated that "cryptocurrency kiosk operators—also considered MSBs in the United States—often do not comply with regulations requiring the implementation of AML/CFT programs, including identification and reporting of suspicious transactions, despite the fact that such kiosks have been linked to illicit use by drug dealers, credit card fraud schemers, prostitution rings, and unlicensed virtual asset exchangers."[374]

FinCEN has provided a series of indicators that indicate elevated risk of illicit activity through CVC Kiosks, including:

- A customer operates multiple CVC kiosks in locations that have a relatively high incidence of criminal activity.
- Large numbers of transactions from different customers sent to and from the same CVC wallet address but not operating as a known CVC exchange.
- Structuring of transactions just beneath the CTR threshold or the CVC kiosk daily limit to the same wallet address either by using multiple machines (i.e., smurfing) or multiple identities tied to the same phone number.[375]

Industry guidance has identified additional CVC Kiosk-related indicators, including:

- Transfers from different cities, as this may be an indicator for human trafficking. Human traffickers are often constantly touring different cities and may need to pay for advertisements using digital assets.
- A high percentage of a customer's activity is limited to CVC ATM withdrawals.
- CVC ATM withdrawals are detected as occurring in areas with high crime rates, particularly human trafficking and drug trafficking.
- A customer uses virtual currency ATMs located at physical addresses associated with what appear to be front businesses, and which may themselves be owned by criminals complicit in the illegal activity.
- A single front business displays turnover levels that are implausibly high.[376,377]

[374] Department of Justice: Attorney General's Cyber-Digital Task Force, "DOJ released 'Cryptocurrency: An Enforcement Framework'" (October 2020).

[375] See "Red Flag Indicators of the Abuse of Virtual Currencies" section of FinCEN's "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 2019).

[376] See Sections 6.8 from Project Participate's "Indicators of Suspicion for Virtual Asset Service Providers" (2019).

[377] See Part 4 of Elliptic's "Money Laundering & Terrorist Financing Typologies in Cryptocurrencies" (March 2020).

Attempted Concealing of Identity and Source of Funds

The digital asset space faces increased challenges when onboarding customers due to the online nature of most customer onboarding. DDs should be observant to attempts to conceal identities through incomplete, unverifiable, or fraudulent documentation. Such activity is of particular concern in the case of potential hackers who have gained access to personal information and attempt to onboard using said identities. When criminals or their mules are able to access legitimate exchanges, it has a 'mixing' effect due to the use of omnibus accounts. For example, the use of "mixers" or "tumblers" has been popular among illicit actors to facilitate financial crimes, as they obfuscate the source or owner of cryptocurrency by mixing the currencies of several users prior to delivery.[378]

Industry guidance has identified indicators for attempts to conceal identify and source of funds, including:

- A customer provides unusual or suspicious identification documents that cannot be readily verified, such as low-resolution identity documents, documents in non-Roman characters, and utility bills and DD statements from unknown or niche companies.
- A customer fails to provide additional information upon request, or is reluctant to provide information or provides inconsistent information.
- A customer takes an inordinate amount of time to provide requested documents.
- Hackers who have gained access to photographs may try to reuse these pictures to register hacker-controlled accounts.
    - Instances when the note on a selfie used for registration looks irregular. Sometimes hackers will obtain selfie photos from previous account registrations and manipulate the notes to use them for a new registration.
    - Instances when the hand, ID or note on a selfie looks irregularly juxtaposed on a picture.
- The alignment of graphics behind the text of identification document ("IDs"). Fraudsters may need to alter the background graphics of an ID as they change the name, address, date of birth ("DOB") or other text in an ID.
- Source of funds documents supposedly in the name of a spouse.
- Source of funds documents that are screen-captures of wallet balances with no identifying information, such as the client name.
- Large numbers of accounts opened simultaneously by groups of foreign nationals, who may be exploited for the purposes of opening accounts, and who have no clear link to the country where the exchange operates.

[378] Department of Justice: Attorney General's Cyber-Digital Task Force, "DOJ released 'Cryptocurrency: An Enforcement Framework'" (October 2020).

- Instances where there are inconsistencies between the customer's stated identifying information and other data they provide or activity they undertake.[379,380]
- "Hopping" between blockchains.

Privacy Coins

Privacy coins refer to "cryptocurrencies that integrate anonymizing techniques (such as the use of stealth addresses, ring signatures, or zk-SNARKs) as part of their design and that feature blockchains that do not reveal full details of counterparties and transactions."[381] There are potentially legitimate purposes for such products, such as IT security or privacy absent criminal activity. A potential mitigating factor that DDs should consider is the willingness of a customer to provide identifying information and transaction data relating to privacy coins at the request of the DD. In addition to privacy coins, there has been an increased use of anonymity-enhanced cryptocurrencies and anonymity-enhancing technology, which—like privacy coins—obfuscate the source or owner of cryptocurrency.[382]

This typology may also include the rapid conversion of a more traditional digital asset to a privacy coin which is then withdrawn. Industry guidance has identified privacy coin-related indicators, including:

- A customer who transacts in privacy coins without using other trading services.
- A customer who transacts with privacy coins and completes trades using privacy coins that appear to be reckless or economically irrational.
- A customer deposits a privacy coin and converts deposit into a more traditional cryptocurrency and subsequently withdraws funds in a short time frame (e.g., high velocity traditional cryptocurrency to privacy coin conversions).[383]

Privacy Wallets

Privacy wallets combine security features like encryption and IP address anonymization with tools to obfuscate crypto transaction trails.[384] Similar to privacy coins, there are potentially legitimate

---

[379] See Sections 6.1 from Project Participate's "Indicators of Suspicion for Virtual Asset Service Providers" (2019).

[380] See Part 1.3 of Elliptic's "Money Laundering & Terrorist Financing Typologies in Cryptocurrencies" (March 2020).

[381] See Part 10 of Elliptic's "Money Laundering & Terrorist Financing Typologies in Cryptocurrencies" (March 2020).

[382] Department of Justice: Attorney General's Cyber-Digital Task Force, "DOJ released 'Cryptocurrency: An Enforcement Framework'" (October 2020).

[383] See Sections 6.4 from Project Participate's "Indicators of Suspicion for Virtual Asset Service Providers" (2019).

[384] Certified Financial Crime Specialists "Privacy Wallets and Crypto Crime – A Top Trend in Illicit Use of Cryptocurrencies" (February 2021).

purposes for using privacy wallets, such as for IT security or privacy absent criminal activity. However, data from the blockchain shows that criminals have been exploiting privacy wallets for illicit activity and that, over the last couple of years, the use of privacy wallets by illicit actors (e.g., in money laundering) has trended upwards, becoming more popular and appealing to financial criminals than mixers and tumblers.[385] A potential mitigating factor that DDs should consider is the willingness of a customer to provide identifying information and transaction data relating to privacy wallets at the request of the DD. Privacy wallet-related indicators include:

- A customer who uses a privacy wallet without using other trading services.
- A customer who uses a privacy wallet in transactions that appear to be reckless or economically irrational.
- A customer who uses a privacy wallet to make high velocity transactions/conversions and/or whose use of a privacy wallet is suggestive of a peeling chain typology[386].

Online Gambling and Gaming

Online gambling sites that accept digital assets often allow a user to 'cash-out' the relevant digital asset for fiat currency after a small number of transactions, often with limited or absent KYC processes. This facilitates the ability to convert proceeds of illicit activity through such sites as digital asset ATMs. Users should be monitored for connections to such sites, particularly when occurring at high volumes. Similarly, many online game currencies can be exchanged for digital assets leading to the same concerns. Furthermore, there has been a growth of virtual-currency-based "casinos" that facilitate various forms of betting denominated in bitcoin and other virtual currencies, which obfuscate the source or owner of cryptocurrency and allow illicit actors to take advantage of such virtual currency casinos in the absence of appropriate AML and OFAC/sanctions controls to mitigate risk.[387]

- A customer makes use of unlicensed, unregulated, or Tor-based gambling.
- A customer makes frequent use of online gambling sites that do not require any KYC and make an open commitment to protecting anonymity of users.
- A customer makes use of gambling sites that do not publish information about their ownership or their jurisdiction of registration.
- A customer makes use of gambling sites that do not impose limits on volumes and values of virtual currency used.

---

[385] Elliptic "Over 13% of all Proceeds of Crime in Bitcoin are Now Laundered Through Privacy Wallets" (December 2020).

[386] A peeling chain is a common money laundering technique associated with digital assets where the transaction activity recorded on-chain indicates an effort to launder a large sum of digital assets through a series of minor transactions.

[387] Department of Justice: Attorney General's Cyber-Digital Task Force, "DOJ released 'Cryptocurrency: An Enforcement Framework'" (October 2020).

- A customer deposits/receives large volumes/values of digital assets over a short time period at an exchange that facilitates swaps with in-game currencies.
- A customer is unable to explain why they require virtual currency to in-game currency swaps of such a significant value.[388,389]

Decentralized Exchanges

Decentralized exchanges allow virtual currency-to-virtual currency exchanges in real time through the use of smart contracts. While the non-custodial nature of such exchanges may reduce the risk of theft, they also present opportunities for illicit activity by avoiding KYC requirements and administrative oversight associated with covered financial institutions.

Industry guidance has identified decentralized exchange-related indicators, including:

- A customer suddenly receives a large amount of virtual currency directly from a decentralized exchange-associated account and attempts to cash out immediately.
- A customer cannot provide evidence or logical explanation for their source of funds.
- The decentralized exchange in question may be associated with relatively high volumes of illicit activity involving dark marketplaces, exchange hacks, and other crimes such as ransomware attacks.[390,391]

[388] See Parts 5.1 and 5.2 of Elliptic's "Money Laundering & Terrorist Financing Typologies in Cryptocurrencies" (March 2020).

[389] See McAfee Labs White Paper "Jackpot! Money Laundering Through Online Casinos" (April 2014).

[390] See Part 3 of Elliptic's "Money Laundering & Terrorist Financing Typologies in Cryptocurrencies" (March 2020).

[391] FinCEN, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" (November 2021).

Appendix C: DD Request Letter Items

As part of the examination planning process, the examiner should prepare a request letter. The list below includes materials that examiners *may* request or request access to for a DD AML/CFT examination. This list should be tailored for the specific DD's risk profile and the planned examination scope. Additional materials may be requested as needed.

The items below are presented in the order they appear in this Examination Manual, and are followed by additional core and expanded sections captured in the FFIEC manual.

DD Core Examination Overview and Procedures

BSA/ AML Risk Assessment

- Make available copies of management's AML/CFT risk assessment of products, services, customers, and geographic locations.
- Make available copies of the DD's policies, procedures, and processes used to conduct the DD's AML/CFT risk assessment.
- List of the DD's identified higher-risk accounts.

OFAC Risk Assessment

- Make available copies of management's OFAC risk assessment of products, services, customers, geographic locations, and distribution channels.
- Make available copies of the DD's policies, procedures, and processes used to conduct the DD's OFAC risk assessment.

AML/CFT Compliance Program

- Make available copies of the most recent written AML/CFT compliance program approved by board of directors (or the statutory equivalent of such a program for foreign financial institutions operating in the United States), including CIP requirements, with date of approval noted in the minutes.
- Make available copies of the policy and procedures relating to all reporting and recordkeeping requirements, including suspicious activity reporting.
- Correspondence addressed between the DD, its personnel or agents, and its federal and state banking agencies, the U.S. Treasury (Office of the Secretary and U.S. Department of the Treasury, IRS, FinCEN, and OFAC) or law enforcement authorities since the previous AML/CFT examination.

BSA/ AML Internal Controls

- Provide the DD's policies, procedures, and processes relevant for AML/CFT internal controls (including but not limited to: onboarding, KYC, CDD/EDD, transaction monitoring, issues management, quality assurance, and regulatory reporting).

- Provide at least three consecutive management information systems reports of AML/CFT and OFAC-related key risk indicators ("KRIs"), status of any open issues and associated management corrective actions, and relevant escalations to senior management and the board.

BSA/ AML Independent Testing

- Make available copies of the results of any internally or externally sourced independent audits or tests performed since the previous examination for AML/CFT, including the scope or engagement letter, management's responses, and access to the workpapers.
- Make available access to the auditor's risk assessment, audit plan (schedule), and program used for the audits or tests.

BSA/ AML Compliance Officer

- Name and title of the designated BSA compliance officer and, if different, the name and title of the person responsible for monitoring AML/CFT compliance.
  - Organization charts showing direct and indirect reporting lines.
  - Copies of résumés and qualifications of person(s) serving in AML/CFT compliance program oversight capacities.

BSA/ AML Training

- Training documentation (e.g., materials used for training since the previous AML/CFT examination including any digital assets-specific trainings).
- AML/CFT training schedule with dates, attendees, and topics. A list of persons in positions for which the DD typically requires AML/CFT training but who did not participate in the training.

Assessing the OFAC Compliance Program

- Make available copies of OFAC policies and procedures.
- Make available a list of blocked or rejected transactions with individuals or entities on the OFAC list and reported to OFAC. *(All blocked transactions must be reported to OFAC within ten business days by filing a Report of Blocked Transactions.)*
- If maintained, make available logs or other documentation related to reviewing potential OFAC matches, including the method for reviewing and clearing those determined not to be matches.
- Provide a list of any OFAC licenses issued to the DD. *(OFAC has the authority, through a licensing process, to permit certain transactions that would otherwise be prohibited under its regulations. If a DD's customer claims to have a specific license, the DD should verify that the transaction conforms to the terms of the license and obtain a copy of the authorizing license.)*
- Provide a copy of the Annual Report of Blocked Property submitted to OFAC (TD F 90-22.50). *(A report of all blocked assets must be provided to OFAC annually by September*

30.)

OFAC Management Commitment

- Name and title of the designated OFAC compliance officer and, if different, the name and title of the person responsible for monitoring OFAC compliance.
- Organization charts showing direct and indirect reporting lines.
- Copies of résumés and qualifications of person (or persons) serving in OFAC compliance program oversight capacities.
- Provide any relevant minutes from the board of directors and senior management regarding the development of the OFAC Compliance Program.

OFAC Internal Controls

- Provide the DD's policies, procedures, and processes relevant for OFAC internal controls (including but not limited to: sanctions screening at onboarding, ongoing screening, issues management, quality assurance, and regulatory reporting).
- Provide access to new accounts across the DD's offerings, including any relevant OFAC searches performed on said customers.
- Provide access to false hits (potential matches), and any associated records evidencing review.
- If applicable, provide a copy of the records verifying that the most recent updates to OFAC software have been installed.

OFAC Independent Testing

- Make available copies of the results of any internally or externally sourced independent audits or tests performed since the previous examination for OFAC, including the scope or engagement letter, management's responses, and access to the workpapers.
- Make available access to the auditor's risk assessment, audit plan (schedule), and program used for the audits or tests.

OFAC Training

- Training documentation (e.g., materials used for training since the previous OFAC examination including any digital assets-specific trainings).
- OFAC training schedule with dates, attendees, and topics. A list of persons in positions for which the DD typically requires OFAC training but who did not participate in the training.

Assessing Compliance with BSA Regulatory Requirements Examination Procedures

Customer Identification Program

- List of accounts without taxpayer identification numbers (TIN).

- File of correspondence requesting TINs for DD customers.
- A copy of any account opening forms (e.g., for loans, deposits or other accounts) used to document CIP/Customer Due Diligence information.
- Written description of the DD's rationale for CIP exemptions for existing customers who open new accounts.
- List of new accounts covering all product lines (including accounts opened by third parties) and segregating existing customer accounts from new customers, for

  _____. *(Examiner to insert a period of time appropriate for the size and complexity of the DD.)*

- List of any accounts opened for a customer that provides an application for a TIN.
- List of any accounts opened in which verification has not been completed or any accounts opened with exceptions to the CIP.
- List of customers or potential customers for whom the DD took adverse action,[392] on the basis of its CIP.
- List of all documentary and nondocumentary methods the DD uses to verify a customer's identity.
- Make available customer notices and a description of their timing and delivery, by product.
- List of the financial institutions on which the DD is relying, if the DD is using the "reliance provision." The list should note if the relied-upon financial institutions are subject to a rule implementing the AML/CFT compliance program requirements of 31 USC 5318(h) and are regulated by a federal functional regulator.
- Provide the following:
  - Copies of any contracts signed between the parties.
  - Copies of the CIP or procedures used by the other party.
  - Any certifications made by the other party.
- Copies of contracts with financial institutions and with third parties that perform all or any part of the DD's CIP.
- Make available copies of the policies, procedures, and processes related to the DD's Customer Identification Program. These should include any identity verification tools or solutions used by the DD.

Customer Due Diligence

- Make available copies of the policies, procedures, and processes related to performing Customer Due Diligence. These should include the customer risk rating methodology and any specialized and/or enhanced due diligence processes.

[392] As defined by 12 CFR 202.2(c).

Suspicious Activity Reporting

- Access to SARs filed with FinCEN during the review period and the supporting documentation. Include copies of any filed SARs that were related to section 314(a) requests for information or to section 314(b) information sharing requests.
- Any analyses or documentation of any activity for which a SAR was considered but not filed, or for which the DD is actively considering filing a SAR.
- Description of expanded monitoring procedures applied to higher-risk accounts.
- Determination of whether the DD uses a manual or an automated account monitoring system(s), or a combination of the two for fiat-based and digital asset activity. If an automated system is used, determine whether the system is proprietary or vendor supplied.
- Make available copies of reports used for identification of and monitoring for suspicious transactions. These reports include, but are not limited to, suspected kiting reports, currency activity reports, monetary instrument records, digital asset analytics records, and funds transfer reports. These reports can be generated from specialized AML/CFT software, the DD's general data processing systems, or both.
- If not already provided, copies of other reports that can pinpoint unusual transactions warranting further review that the DD maintains. Examples include nonsufficient funds (NSF) reports, account analysis fee income reports, source of funds reports, and large item reports.
- Provide name, purpose, parameters, and frequency of each report.
- Correspondence received from federal law enforcement authorities concerning the disposition of accounts reported for suspicious activity.
- Make available copies (or a log) of criminal subpoenas received by the DD since the previous examination or inspection.
- Make available copies of policies, procedures, and processes used to comply with all criminal subpoenas, including National Security Letters (NSL), related to BSA.

Currency Transaction Reporting

- Access to filed Currency Transaction Reports (CTR) for the review period.
- Access to internal reports used to identify reportable currency transactions for the review period.
- List of products or services that may involve currency transactions.

New Products, Processes, and Technologies

- Make available the DD's process for identifying when a product, practice, and/or technology should be treated as 'new', or a new technology is used for an existing or new product or service offering.
- Provide policies, procedures, and processes related to the assessment and mitigation of the ML/TF and sanctions risks posed by new products, practices, and technologies, including all digital assets supported by the DD.
- Make available a list of any products, practices, and/or technologies that have been

identified as 'new' or have been added since the last examination. The list should include a description of the relevant products, processes, and technologies, as well as the date they were released into production.

Digital Asset Analytics

- Make available policies, procedures, and processes related to digital asset analytics. If the system was provided by an outside vendor, request (i) a list that includes the vendor, (ii) application names, and (iii) installation dates of any digital asset analytics system provided by an external vendor. Request a list of the algorithms or rules used by the systems and copies of the independent validation of the software against these rules.
- Make available model documentation for any digital asset analytics technologies in use, including description of the methodology employed.
- Make available copies of records and alerts generated by digital asset analytics technology.
- Make available service level agreements as warranted.

Virtual Currency Funds Transfers Recordkeeping

- Make available copies of the DD's policies, processes, and procedures around transaction data collection requirements for all virtual currencies supported by the DD, including data governance processes around how these records are maintained, and integrated into the DD's overall control framework.
- Make available records of digital assets funds transfers, including incoming, intermediary, and outgoing transfers for all virtual currencies and stablecoins offered, issued, or supported by the DD by applicable breakdowns (e.g., by jurisdiction or customer) as otherwise required by law.

Model Risk Management

- Make available processes, practices, and procedures related to model risk management.
- Make available any AML/CFT and/or OFAC tools and associated documentation that are classified as models from the DD's model inventory.
- Provide the most recent independent validation report and associated testing for each AML/CFT and OFAC model.
- Provide any findings identified during the course of independent validations and any actions taken in response to these potential findings.
- Evidence supporting the qualifications and reporting structure for validation teams.

BSA and OFAC Record Retention Requirements

- Make available the DD's policies, processes, and procedures around record retention requirements, including record retention schedule.

Product Examination Procedures

On-off Ramp Exchange and Virtual Fund Transfers

- Make available the DD's policies, procedures, and processes related to virtual currency funds transfers.
- Provide the processes in place to screen customer information for each originator and beneficiary for each type of virtual currency transaction (including virtual currency on-ramps, virtual currency off-ramps, and external virtual currency transfers *for* ***each virtual currency*** that the DD offers).
- Make available the DD's policies, procedures, and processes related to risk profiling counterparties.
- Make available virtual currency funds transfer activity for each virtual currency the DD offers.

Staking-as-a-Service for DDs

- Make available the DD's policies, procedures, and processes related to the DD's staking-as-a-service operations.
- Provide any high-risk staking-as-a-service customers and associated EDD.

Digital Asset Escrow Services

- Make available the DD's policies, procedures, and processes related to the DD's digital assets escrow services.
- Provide policies, procedures, and processes related to gathering additional identification information about the settlor, grantor, trustee, or other persons with authority to direct a trustee, in order to establish the true identity of the customer.
- Provide documentation regarding any monitoring systems in use for digital assets escrow services.
- Access to digital asset escrow relationships and associated due diligence documentation.

Stablecoin Networks

- Make available the DD's policies, procedures, and processes related to the DD's stablecoin networks, including access criteria, due diligence, ongoing monitoring, freezing capabilities and compliance with law enforcement requests in the code of any stablecoin tokens that are created.
- Provide members of the stablecoin network considered 'high-risk' along with access to associated transaction activity.

Virtual Currency Automated Teller Machine Owners or Operators

- Provide a risk assessment covering privately owned virtual currency automated teller machines (ATMs), including a list of higher-risk privately owned ATM relationships.

- Make available copies of policies, procedures, and processes for privately owned virtual currency ATMs account acceptance, due diligence, and ongoing monitoring.
- Provide SARs and subpoenas related to privately owned virtual currency ATMs.

Politically Exposed Persons

- Make available copies of policies, procedures, and processes specific to politically exposed persons (PEP). Policies should include the DD's definition of a PEP as well as procedures for opening PEP accounts and senior management's role in the approval process for opening PEP accounts.
- Provide a list of accounts in the name of or for the benefit of a PEP. List should include the country of residence of the PEP, the account balances, and the average number and dollar volume of transactions per month.
- Provide a list of the information systems or other methods used to identify PEP accounts.
- Make available management reports used to monitor PEP accounts, including reports for identifying unusual and suspicious activity.

Charities and Nonprofit Organizations

- Make available copies of policies, procedures, and processes related to charities and nonprofit organizations.
- List of charities and nonprofit organizations, particularly those that the DD has designated as higher risk. This list should include average account balances and the average number and dollar volume of transactions.
- List of nonprofit organizations involved in higher-risk geographic locations.

Correspondent Accounts (Foreign)

- Make available copies of policies, procedures, and processes specifically for foreign correspondent financial institution accounts, including procedures for monitoring for suspicious activity.
- Make available a list of foreign correspondent financial institution accounts.
- Make available a list of the DD's accounts with its foreign branches or overseas subsidiaries and the steps the DD has taken to ensure the accounts with its branches or overseas subsidiaries are not used to indirectly conceal the source, ownership or use of prohibited or illicit funds.
- Provide risk assessments covering foreign correspondent financial institution account relationships, including those with its foreign branches or overseas subsidiaries.
- Provide a list of SARs filed relating to foreign correspondent financial institution accounts.

Private Banking

- Make available copies of policies, procedures, and controls used to manage AML/CFT risks associated with private banking clients (e.g., family offices, high net-worth and ultra high net-worth individuals).

- Make available business or strategic plans for the private banking clients.
- Provide the most recent version of management reports on private banking client activity, such as customer aggregation reports, policy exception reports, client concentrations, customer risk classification reports, and unusual account activity.
- Provide recent private banking client reports from compliance, internal audit, risk management, and external auditors or consultants that cover AML/CFT.
- Provide a list of products and services offered to private banking clients. Information on new products and services offered to private banking clients and the DD's process for approving new activities.
- Provide a description of the method for aggregating customer holdings and activities across business units throughout the organization.
- Provide a description of account officer and manager positions, and the compensation, recruitment, and training program for these positions.
- Make available the code of ethics policy for private banking officers.
- Provide a risk assessment covering private banking customers and transactions.
- Provide a list of suspense, concentration, or omnibus accounts used for private banking transactions. Describe the purpose for each account and the controls governing it.
- Provide management reports covering 25 to 50 of the largest, most active, or most profitable private banking customers.
- Provide a list of the DD's private banking accountholders who meet the following criteria:
    - Politically exposed persons (PEP), export or import business owners, money transmitters, Private Investment Companies (PIC), financial advisers, offshore entities, or money managers (when an intermediary is acting on behalf of customers).
    - Customers who were introduced to the DD by individuals previously employed by other financial institutions.
    - Customers who were introduced to the DD by a third-party investment adviser.
    - Customers who use nominee names.
    - Customers who are from, or do business with, a higher-risk geographic location.
    - Customers who are involved in cash-intensive businesses.
    - Customers who were granted exceptions to policies, procedures, and controls.
    - Customers who frequently appear on unusual activity monitoring reports.
- Provide SARs and subpoenas related to private banking clients.
- Make available a copy of account-opening documentation or agreements for private banking clients.

Nonbank Financial Institutions

- Make available copies of policies, procedures, and processes related to nonbank financial institutions (NBFIs).
- Provide a list of NBFI accounts, including all related accounts.
- Provide a risk assessment of NBFI accounts, identifying those accounts the DD has designated as higher risk. This list should include products and services offered by the

NBFI; the average account balance; and the average number, type, and dollar volume of transactions per month.
- Provide a list of foreign nonbank financial institution accounts, including the products and services offered; the average account balance; and the average, number, type, and dollar volume of transactions per month.
- Provide a sample of account opening documentation for higher-risk NBFI.
- Provide a list of SARs and subpoenas related to NBFI.

Business Entities (Domestic and Foreign)

- Make available copies of policies, procedures, and processes specifically related to domestic and international business entities.
- Provide a list of accounts opened by business entities. If this list is unreasonably long, amend the request to look at those entities incorporated in higher-risk jurisdictions or those accounts the DD has designated as higher risk.
- Provide a list of business entities that identify as DAOs; include in this list the purpose of the DAO, and any relevant due diligence information.

FFIEC Core Examination Procedures

Beneficial Ownership (FFIEC AML Manual)

- Make available copies of the DD's policies, procedures, and processes related to collection of beneficial ownership information (to the degree these are not currently included above).

Currency Transaction Reporting Exemptions (FFIEC AML Manual)

- Access to filed Designation of Exempt Person report(s)(s) for current exemptions.
- List of customers exempted from CTR filing and the documentation to support the exemption (e.g., currency transaction history or, as applicable, risk-based analysis).
- Access to documentation of required annual reviews for CTR exemptions.

Information Sharing (FFIEC AML Manual)

- Documentation of any positive match for a section 314(a) request.
- Make available documentation demonstrating that required searches have been performed.
- Make available any vendor-confidentiality agreements regarding section 314(a) services, if applicable.
- Make available copies of policies, procedures, and processes for complying with 31 CFR 1010.520 (Information Sharing Between Federal Law Enforcement Agencies and Financial Institutions).
- If applicable, a copy of the DD's most recent notification form to voluntarily share information with other financial institutions under 31 CFR 1010.540 (Voluntary

Information Sharing Among Financial Institutions), i.e., section 314(b) information sharing, or a copy of the most recent correspondence received from FinCEN that acknowledges FinCEN's receipt of the DD's notice to voluntarily share information with other financial institutions.
- If applicable, make available copies of policies, procedures, and processes for complying with 31 CFR 1010.540 (i.e., section 314(b) information sharing).

Purchase and Sale of Monetary Instruments (FFIEC AML Manual)

- Access to records of sales of monetary instruments in amounts between $3,000 and $10,000 (if maintained with individual transactions, provide samples of the record made in connection with the sale of each type of monetary instrument).

Funds Transfers Recordkeeping (FFIEC AML Manual)

- Access to records of funds transfers, including incoming, intermediary, and outgoing transfers of $3,000 or more.

Foreign Correspondent Account Recordkeeping, Reporting and Due Diligence (FFIEC AML Manual)

- List of all foreign correspondent bank accounts, including a list of foreign financial institutions, for which the DD provides or provided regular services, and the date on which the required information was received (either by completion of a certification or by other means).
- If applicable, documentation to evidence compliance with 31 CFR 1010.630 (Prohibition on Correspondent Accounts for Foreign Shell Banks; Records Concerning Owners of Foreign Banks and Agents for Service of Legal Process) and 31 CFR 1010.670 (Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationship) (for foreign correspondent bank accounts and shell banks).
- List of all payable through relationships with foreign financial institutions as defined in 31 CFR 1010.605.
- Access to contracts or agreements with foreign financial institutions that have payable through accounts.
- List of the DD's foreign branches and the steps the DD has taken to determine whether the accounts with its branches are not used to indirectly provide services to foreign shell banks.
- List of all foreign correspondent bank accounts and relationships with foreign financial institutions that have been closed or terminated in compliance with the conditions in 31 CFR 1010.630 (i.e., service to foreign shell banks, records of owners and agents).
- List of foreign correspondent bank accounts that have been the subject of a 31 CFR 1010.520 (Information Sharing Between Federal Law Enforcement Agencies and Financial Institutions) or any other information request from a federal law enforcement officer for information regarding foreign correspondent bank accounts and evidence of

compliance.
- Any notice to close foreign correspondent bank accounts from the Secretary of the Treasury or the U.S. Attorney General and evidence of compliance.
- Make available copies of policies, procedures, and processes for complying with 31 CFR 1010.630.
- List of all the DD's embassy or consulate accounts, or other accounts maintained by a foreign government, foreign embassy, or foreign political figure.
- List of all accountholders and borrowers domiciled outside the United States, including those with U.S. power of attorney.

FFIEC Expanded Examination Procedures

Funds Transfers (FFIEC AML Manual)

- Provide funds transfer activity logs, including funds transfers that involve cover payments, including transfers into and out of the DD. Include the number and dollar volume of funds transfer activity for the month.
- Provide a list of funds transfers purchased with currency over a specified time period.
- Provide a list of noncustomer transactions over a specified time period.
- If not already included in the AML/CFT policies, make available copies of any policies, procedures, and processes related to funds transfers, including transfers that involve cover payments, or payable upon proper identification (PUPID).
- Provide a list of suspense accounts used for PUPID proceeds.
- Provide a list of PUPID transactions completed by the DD, either as the beneficiary DD or as the originating DD.
- Make available SWIFT messages (i.e., foreign exchange confirmations, debit and credit entry confirmations, statements, collections and documentary credits).

Automated Clearing House Transactions (FFIEC AML Manual)

- Make available copies of any policies and procedures related directly to automated clearing house (ACH) and international ACH transactions (IAT) that are not already included in the AML/CFT policies.
- Make available copies of management reports that indicate the monthly volume of ACH activity, including IATs.
- Make available a list of large or frequent ACH transactions or IATs.
- Make available correspondence from NACHA.
- Make available a list of IATs (both those originated from or received by the DD).
- Make available a list of customer complaints regarding ACH transactions and IATs.

Purchase and Sale of Monetary Instruments (FFIEC AML Manual)

- If not already included in the AML/CFT policies, make available copies of any policies, procedures, and processes related to the sale of monetary instruments for currency. In

particular, include policies, procedures, and processes related to the monitoring sales of monetary instruments in order to detect unusual activities.
- Provide monetary instrument logs or other MIS reports used for the monitoring and detection of unusual or suspicious activities relating to the sales of monetary instruments.
- Provide a list of noncustomer transactions over a specified period of time.
- Provide a list of monetary instruments purchased with currency over a specified time period.
- Provide a list of SARs filed related to the purchase or sale of monetary instruments.

Nondeposit Investment Products (FFIEC AML Manual)

- Make available copies of policies, procedures, and processes relating to nondeposit investment products (NDIP) and relationships with any independent NDIP providers.
- Provide internal audits covering NDIP sales and provider relationships.
- Provide a risk assessment covering NDIP customers and transactions.
- If available, provide a list of NDIP clients and balances.
- Provide a list of suspense, concentration, or omnibus accounts used for NDIP. Describe the purpose for and controls surrounding each account.
- Provide management reports covering 25 to 50 of the largest, most active, and most profitable NDIP customers.
- Provide SARs and subpoenas related to NDIP customers.
- Make available a copy of account opening documentation or agreements for NDIP.
- Make available a copy of contracts or agreements between the DD and third-party NDIP providers for the completion of CIP, due diligence, and ongoing monitoring of NDIP customers.

Nonresident Aliens and Foreign Individuals (FFIEC AML Manual)

- Make available copies of policies, procedures, and processes specific to nonresident alien (NRA) accounts, including guidelines and systems for establishing and updating W-8 exempt status.
- Provide a list of NRA and foreign individual accounts held by the DD, particularly those accounts the DD has designated as high risk.
- Provide a list of NRA and foreign individual accounts without a TIN, passport number, or other appropriate identification number.
- Provide a list of SARs and subpoenas related to NRA and foreign individual accounts.

DD Internal Audit Testing Matrix

Note – as part of Internal Audit requests, The Department may request a testing matrix of areas that the DD's internal audit function has reviewed.

Review Area	Sampling Size (# of Items Tested)	Sample Universe (Population Size)	Sample/Test Period	Sampling/Testing Rationale
CIP (31 CFR 1020.100)				
CDD / EDD (or number of customers by risk rating, including customers subject to EDD)				
Section 311 - Special Measures				
Sections 314(a) & 314(b) - Information Requests				
Transaction Monitoring - Automated: Alerts/Cases (e.g., volume of alerts and cases)				
SAR Approval and Filing Process for BSA and non-BSA cases				
OFAC - Customers/Related Parties - Onboarding				
OFAC - Customers/Related Parties - Periodic Screening/Scrubs				
OFAC - Transactions - Real Time Screening				
OFAC - Blocked Accounts / Rejected Transactions				
OFAC - System - Filter Updates				
Travel Rule (31 CFR 1010.410) for funds transfers				
Travel Rule (31 CFR 1010.410) for virtual currency funds transfers				
Other				

Appendix D. Abbreviations and Key Terms

Abbreviation or Term	Full Name or Description
ACH	Automated Clearing House
AEC	Anonymity Enhanced Cryptocurrency
AI	Artificial Intelligence
AML	Anti-Money Laundering
BSA	Bank Secrecy Act
CDD	Customer Due Diligence
CFR	Code of Federal Regulations
CIF	Customer Information File
CIP	Customer Identification Program
CTR	Currency Transaction Report
CVC	Convertible Virtual Currency
Digital Asset (or "controllable electronic record" per NRS-8-3003 (5))	A digital asset that is used or bought primarily for consumptive, personal or household purposes and includes: (A)An open blockchain token constituting intangible personal property as otherwise provided by law; (B)Any other digital asset which does not fall within the definitions of digital security or virtual currency. Per Nebraska legislation, the term digital asset has the same meaning as 'controllable electronic record', and does not include electronic chattel paper, electronic documents, investment property, and transferable records under the Uniform Electronic Transactions Act.
DAO	Decentralized Autonomous Organization
DD	Digital Asset Depository Institution
DEX	Decentralized Exchange
DeFi	Decentralized Finance
EDD	Enhanced Due Diligence
EIC	Examiner in Charge
FATF	Financial Action Task Force on Money Laundering
FAQ	Frequently Asked Question
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Financial Crimes Enforcement Network
GO	Gateway Operator
HIDTA	High Intensity Drug Trafficking Area
HIFCA	High Intensity Financial Crime Area
INCSR	International Narcotics Control Strategy Report
IAT	International ACH Transaction
IP	Internet Protocol
JMLSG	Joint Money Laundering Steering Group
KPI	Key Performance Indicator
KRI	Key Risk Indicator
KYC	Know Your Customer

LLC	Limited Liability Company
LTDA	Legal tender digital asset
ML/TF	Money Laundering / Terrorist Financing
MIS	Management Information Systems
MRM	Model Risk Management
MSB	Money Service Business
NACHA	National Automated Clearing House Association
NCUA	National Credit Union Administration
NFA	National Futures Association
NFIA	Nebraska Financial Innovation Act
NFT	Non-fungible token
NRA	Nonresident Alien
NSL	National Security Letter
NSF	Nonsufficient funds
OCC	Office of the Comptroller of the Currency
ODFI	Originating Depository Financial Institution
OFAC	Office of Foreign Assets Control
OFC	Offshore Financial Center
P2P	Peer-to-Peer
PEP	Politically Exposed Person
PIC	Private Investment Company
RDFI	Receiving Depository Financial Institution
ROE	Reports of Examination
SAR	Suspicious Activity Report
SCP	Sanctions Compliance Program
SDN	Specially Designated Nationals and Blocked Persons
Tor	The Onion Router
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
VASP	Virtual Asset Service Provider
Virtual Currency	A digital asset that is: (A) Used as a medium of exchange, unit of account or store of value; and (B) Not recognized as legal tender by the United States government. Note: Virtual currency or a digital security, as defined in W.S. 34-29-101(a), shall not constitute an open blockchain token.
VPN	Virtual Private Network