



Anti-Money Laundering Guidance

Overview of U.S. Requirements Applicable to
Digital Assets Businesses
July 2022



Preface/ Objective

The following overview of U.S. anti-money laundering regulation intends to provide an overview of the key AML requirements for a Global DCA member for educational purposes and is not intended as legal advice. While it is based on, and reflects, U.S. law, this overview can serve as a good basis to assess and review your AML policies and procedures since the U.S. has one of the strictest AML regimes in the world. The terminology used in this document is the U.S. Treasury's Financial Crimes Enforcement Network ("FinCEN") terminology, which is the bureau that administers the Bank Secrecy Act and other anti-money laundering ("AML") laws in the U.S.

Who is Covered

In 2013 FinCEN first issued an advisory on "virtual currencies",¹ which were defined as a medium of exchange that can operate like a currency but does not have all the attributes of a "real" currency. That would include crypto, digital, virtual, and synthetic, currencies, tokens or assets. The terminology is not dispositive and can collectively be referred to as Convertible Virtual Currency ("CVC").² The people who deal or own these virtual currencies or CVCs can be categorized as either users, or administrators, or exchangers. Users of CVCs are generally not subject to the U.S. AML laws. Administrators (i.e., platform operators) and exchangers (i.e., dealers) are called money transmitters and therefore considered money services businesses (MSBs") subject to the AML laws.

Banks, SEC registered entities and CFTC registered entities are exempt from the definition and requirements of MSBs. They have their own AML obligations enforced by their respective regulators.³ Foreign entities that would be required to register with the SEC or CFTC if located in the U.S. are also exempt from the MSB definition.

¹ Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (March 18, 2013). <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>

² It is important to note the designation of something as a "virtual currency", a crypto currency, or digital asset or the like is a matter of law and therefore outside of the scope of this paper.

³ While each specific U.S. regulator provides specific requirements for their registrants, those regulations are governed by, and for the most part a codification of, general laws such as the Banking Secrecy Act and the USA PATRIOT Act.

MSB Requirements

In 2019 FinCEN⁴ offered guidance on how its regulations apply to businesses that transact in CVCs. A business that meets the definition of an MSB must register with FinCEN (Form 107)⁵ and develop and maintain an effective written AML program to comply with various record keeping and reporting requirements.

The following are a few examples of businesses that meet the definition of an MSB and are therefore subject to FinCEN requirements:

- a. P2P Exchangers⁶
- b. CVC Wallets (hosted)
- c. CVC Kiosks and ATMs⁷
- d. CVC transmitters through decentralized application
- e. Anonymity enhanced CVC transactions (tumblers/ mixers)
- f. Payment processing services involving CVC
- g. CVC transmission by casinos

What is Money Laundering?

Money laundering is typically considered the process of disguising the proceeds of a crime and integrating those proceeds into the financial system. Money laundering may also include the movement of clean money through the financial system with the intent to commit a crime in the future, such as terrorism.

In the past, money laundering was a term generally associated with organized crime. However, government regulators have expanded the definition of money laundering to encompass any financial transaction that generates an asset or a value as the

⁴ Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001 (May 09,2019). <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models>

⁵ See https://www.irs.gov/pub/irs-tege/fin107_msbreg.pdf

⁶ Defined as individuals or entities offering to exchange fiat currencies for virtual currencies or one virtual currency for another virtual currency. P2P exchangers usually operate informally, typically advertising and marketing their services through online classified advertisements, online forums, social media, and through word of mouth. P2P exchangers may provide their services online, or may arrange to meet prospective customers in person to purchase or sell virtual currency.

⁷ CVC kiosks (also called bitcoin Automated Teller Machines (ATMs) or crypto ATMs) are ATM-like devices or electronic terminals that allow users to exchange cash and virtual currency. CVC kiosks generally facilitate money transmission between a CVC exchange and a customer's wallet or operate as a CVC exchange themselves.

result of an illegal act. Money laundering now includes a wide range of crimes such as tax evasion, false accounting and securities fraud. Money laundering is a Federal crime that can result in significant fines and prison sentences of up to 20 years.

Countering the Financing of Terrorism

After the September 11, 2001 terrorist attacks, Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act (USA PATRIOT Act).⁸ The purpose of the USA PATRIOT Act is to deter and punish terrorist acts in the United States and around the world, and to enhance law enforcement's investigatory tools. The Act requires all entities defined as financial institutions under the Bank Secrecy Act to establish written AML compliance programs, verify customer identity and report suspicious activities. MSBs are included in the definition of financial institutions (31 CFR 1010.100(t)).⁹ In light of the expanded emphasis on terrorism, AML is frequently referred to as AML/CFT (Counter the Financing of Terrorism) and many of the new rules are designed to thwart the funding of terrorism.

AML Regulatory Background

Recognizing and preventing possible money laundering is a top priority for government regulators. As a professional in the money services industry, you play an important role in the global effort to stop illegally obtained monies from entering the U.S. financial system and prevent legally obtained funds from being used to promote criminal activities. Understanding anti-money laundering regulations and staying abreast of rule changes are the cornerstones of an effective AML program.

OFAC Sanctions

In the United States, the U.S. Treasury Department performs a critical role in enhancing national security by implementing economic sanctions against foreign threats, identifying and targeting the financial support networks of national security threats and improving the safeguards of the U.S. financial system. The Treasury's Office of Foreign Assets Control (OFAC) administers and enforces economic and trade sanctions against:

⁸ <https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>

⁹ <https://www.law.cornell.edu/cfr/text/31/1010.100>

- Foreign countries and regimes;
- Terrorists;
- International narcotics traffickers;
- Those engaged in activities related to the proliferation of weapons of mass destruction;
- Other threats to the national security, foreign policy or the economy of the United States, including cyber related activities.

OFAC Sanctions Compliance

OFAC maintains sanctions lists including a list of specially designated nationals and blocked persons (searchable SDN list).¹⁰ Persons and entities in the US are prohibited from doing business with anyone that appears on an OFAC sanctions list. OFAC has recently provided guidance to financial institutions regarding their obligation to maintain a sanctions compliance program and the existence of an adequate risk-based sanctions compliance program will be taken into consideration if a penalty is to be imposed for a sanctions violation.¹¹ The essential elements of a sanctions compliance program are as follows:

- a. Senior management commitment to sanctions compliance;
- b. Risk assessments;
- c. Appropriate internal controls including policies and procedures;
- d. Auditing and testing;
- e. Training of relevant personnel.

OFAC has issued “Sanctions Compliance Guidance for the Virtual Currency Industry” which explains the sanctions programs in detail as they apply to virtual currencies.¹²

FATF

The Financial Action Task Force (FATF), the international AML watchdog, has also issued guidance on the AML/CFT risks associated with what they call virtual asset

¹⁰ <https://sanctionssearch.ofac.treas.gov/>

¹¹ https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf

¹² https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf

¹³ <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>

service providers (VASPs)¹³. FATF recommends that, in addition to the required Know Your Customer/Customer Identification Program (KYC/CIP) information, account numbers and wallet addresses of both the sender and receiver of digital assets be recorded and retained by a VASP. In addition, VASPs should develop programs to address the risks posed by digital assets.

Elements of an AML Compliance Program

The Bank Secrecy Act as it applies to MSBs, specifies four basic elements ("pillars") that are required of every AML compliance program. AML program requirements are not, however, "one size fits all." They should be tailored to a financial institution's specific needs and operations. Let's examine each element of an AML compliance program.

1. AML Program Document

Development of Internal Policies, Procedures and Controls, including:

- A policy statement;
- Implementation of a Customer Identification Program;
- Procedures for detecting and reporting suspicious activity;
- Due diligence and monitoring.

2. Training

Annual AML training for appropriate personnel.

3. AML Compliance Officer

Designation of an AML compliance officer.

4. Testing

Independent testing of the AML compliance program.

AML Program Requirements in Detail

Requirement No. 1(a)

Policy Statement

A firm's AML policy should include a clear and unequivocal statement approved by senior management that the firm is committed to following all applicable laws and regulations to ensure that it does not in any way facilitate money laundering. There must be a requirement that all employees are committed to following the firm's AML policy. The policy statement should also emphasize the consequences to an employee who fails to follow the firm's AML policy, including the potential for dismissal, fines and even imprisonment.

Requirement No. 1(b)

Implementation of a Customer Identification Program

The USA PATRIOT Act requires that you and your firm know who you are doing business with. All regulated firms are responsible for obtaining sufficient information so that they may form a reasonable belief as to the true identity of their individual and business customers.

A Customer Identification Program (CIP) contains the four basic steps shown here.

Obtaining Customer Identification Information

Obtaining customer identification information is the first line of defense in identifying high-risk accounts that may pose a threat of money laundering. At a minimum, the following information must be obtained from the customer:

For an Individual Account:

- Name;
- Date of birth;
- Physical address;
- Identification number (such as social security number or taxpayer ID number, or government-issued picture identification for non-U.S. persons).

For a Business Account:

- Name;
- Address (principal place of business and legal address);
- Government-issued identification number (such as tax identification number).

Verifying Customer Identification Information

There are three general methods used to verify a customer's identity:

- Verification through documents. Example: Driver's license, passport or other government-issued documents.
- Verification through non-documentary methods. Example: Independently crosschecking public databases such as Experian, Equifax or LexisNexis.
- Other verification methods. Example: Reliance on third-party sources to verify customer identity. A financial institution may enter into an agreement to rely on another financial institution's customer identification if the agreement is in writing and certified annually, and the financial institution being relied on is required to have an AML compliance program pursuant to the BSA and is regulated by a Federal functional regulator.

Generally, the verification process must be completed before the account can be opened. If the applicant has applied for but not received a taxpayer identification number, most firms will not open the account until the number has been issued.

If a firm is unable to form a reasonable belief that it knows the true identity of a customer, it should refuse to open the account. If the account has already been opened, further transactions should be limited and the account should be closed.

Additional Verification as Required

Additional verification is usually required for non-U.S. individuals or entities, including foreign financial institutions. Additional verification is also required for "politically exposed persons," (PEPs)

PEPs include heads of state, cabinet ministers, political party leaders, influential executives in nationalized industries or foreign government administration, senior

judicial or military officials and members of ruling families as well as any close associates. OFAC maintains lists of Specially Designated Nationals and Blocked Persons (SDN Lists) as well as a sanctioned countries list and the names and locations of all account applicants must be checked against this list.

The Financial Action Task Force (FATF), issues a quarterly list of high-risk and non-cooperative jurisdictions as well as lists of jurisdictions with strategic AML/CFT deficiencies.¹⁴ The FATF advisory lists those jurisdictions requiring the implementation of counter measures and those jurisdictions requiring enhanced due diligence. FinCEN requires US persons to follow the FATF Advisories and recommendations. The high-risk and non-cooperative jurisdictions are Iran and North Korea. The list of jurisdictions with strategic AML/CFT deficiencies is continually updated. Financial institutions should consider their obligations and risk-based approaches to FATF-identified countries.

In addition to the FATF-listed countries, the EU has established a list of high-risk “third countries” which now follows the FATF list almost exactly.¹⁵ Banks and other financial institutions subject to the EU Anti-Money Laundering Directives must use “enhanced customer due diligence requirements” for transactions involving these high-risk third countries.

Any additional verification that you perform should be delineated in your AML policy and any documents you obtain must be preserved.

Requirement No. 1(c)

Procedure for Detecting and Reporting Suspicious Activity

An essential component of an AML compliance program is the development of procedures designed to detect unusual and suspicious activities. These activities may occur at any point in the life of an account from account opening to account closing. The funding of an account and the withdrawal of funds from an account are frequently areas that need to be monitored.

¹⁴ <https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-march-2022.html>

¹⁵ https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counteracting-financing-terrorism/eu-policy-high-risk-third-countries_en

The trading of an account is also an area that requires vigilance. AML compliance is an obligation of all employees -- including those involved in treasury, finance, settlement and back office operations -- but the person in direct contact with the customer is frequently in the best position to detect suspicious activity at account opening and throughout the life of the account. If you see or hear of something suspicious you should report it to your AML compliance officer.

Requirement No. 1(d)

Due Diligence and Monitoring

An AML compliance program must adhere to several additional requirements:

- FinCEN issues a bi-weekly list of individuals and entities (the confidential 314(a) list)¹⁶ and each MSB must compare these lists to its customer register and report any matches. All reported matches must be kept confidential.
- MSBs must compare their customer registers with the various sanctions lists, including the OFAC lists of Specially Designated Nationals and countries that are under an OFAC-administered sanctions program.
- MSBs must have appropriate, specific, and risk-based due diligence procedures and processes when opening and maintaining correspondent accounts for foreign financial institutions and private banking accounts for non-U.S. persons.

A correspondent account is an account established by a banking institution to handle financial transactions for another financial institution. A private banking account is an account, in excess of \$1 million, opened on behalf of a non-U.S. individual.

¹⁶ <https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf>

Requirement No. 2

Annual Training for All Appropriate Personnel

Firms that are subject to AML requirements are required to provide annual or ongoing AML training to their employees. Firms must maintain records to evidence their compliance with this requirement. The training requirement helps to raise awareness and ensure that the AML program is fully implemented and the appropriate personnel understand current AML rules.

Requirement No. 3

Designation of a Compliance Officer

Firms must have at least one designated AML compliance officer who bears the primary responsibility for ensuring that the firm's AML program is implemented effectively and who oversees day-to-day compliance with the AML program. An AML compliance officer should have in-depth understanding of the firm's business operations, applicable laws and the details of the AML program. The AML compliance officer should report directly to senior management.

Requirement No. 4

Independent Testing of the AML Compliance Program

An individual or group of people who are independent from the compliance department and general flow of money in the firm should be engaged at least annually (every 12 months) to evaluate whether the firm's AML program complies with applicable rules and regulations and is adequate to accomplish the purpose for which it was designed. The independent testing requirement ensures that the success or shortcomings of an AML program are appraised by an unbiased source. The results of the review must be documented and provided to the firm's senior management.

Reporting- Suspicious Activity Reports (SARs)

A report must be filed when a transaction that is conducted by, at or through the MSB is both suspicious, and involves \$2000 or more. A transaction must be reported if the MSB knows, suspects or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

- **Involves funds derived from illegal activity** or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity, or is
- **Designed to evade the requirements of the Bank Secrecy Act**, whether through structuring or other means, or
- **Serves no business or apparent lawful purpose**, and the reporting business knows of no reasonable explanation for the transaction after examining all available facts.
- **Involves use of the money services business** to facilitate criminal activity.

A SAR must be filed through the BSA E-filing system using a SAR MSB form. MSBs have 30 days after becoming aware of a suspicious transaction to complete and file the form. A copy of the filed form and supporting documentation must be retained for a period of five years from the date of filing. MSBs (including MSB employees) are prohibited from disclosing to a person involved in the transaction that a suspicious activity report has been filed. Further, each MSB (including each MSB employee) is protected from civil liability for any SAR filed by the MSB.

Reporting-Currency Transaction Reports (CTRs)

Every MSB must file a report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such MSB which involves a transaction in currency of more than \$10,000. Smaller transactions that have been structured to avoid the \$10,000 threshold may need to be aggregated. Such reports are referred to as CTRs and are filed through the BSA E-filing system within 15 days of the transaction. MSBs must save a copy of the report for five years.


Record Keeping and Reporting –Travel Rule

When an MSB transmits funds equal to or greater than \$3000 to another financial institution there is certain data about the transmitter and the transaction that must be passed along to that financial institution in addition to the funds. The purpose is to create an information trail that law enforcement can use to detect, investigate and prosecute money laundering and other financial crimes.

MSBs must transmit the following data to the recipient financial institution:

The name of the transmittor,

The account number of the transmittor, if used,



The address of the transmittor,
The identity of the transmittor's financial institution,
The amount of the transmittal order,
The execution date of the transmittal order, and
The identity of the recipient's financial institution;

and if received:

The name of the recipient,
The address of the recipient,
The account number of the recipient, and
Any other specific identifier of the recipient.

This information is not reported to the government unless a SAR is warranted. The transmitted information must be retained for five years.