DILENDORF
LAW FIRM

BSA/AML Policies for Cryptocurrency Exchanges and DeFi Applications in a Nutshell

Table Of Contents

BSA/AML Policies for Cryptocurrency Exchanges and DeFi Applications in a Nutshell

Authors: Max Dilendorf, Esq.,and Kareem Tabba

Because cryptocurrency is a value that substitutes for currency, the Financial Crimes Enforcement Network (FinCEN) may classify businesses involved in its exchange or transmission as money transmitters. In fact, most cryptocurrency exchanges and DeFi applications may be considered money transmitters and subject to the laws and regulations governing money services business (MSB) including the Bank Secrecy Act (BSA) which dictates an effective written Anti-Money Laundering (AML) policy. In addition to the mandated AML policy, policies for the federal and state laws and regulations governing MSBs are vital because failing to implement an effective AML policy can lead to civil and criminal charges. And an effective AML policy requires a culture of compliance.

As an example, consider the legalities and questions needing answers when a person opens an account with a cryptocurrency exchange or Defi app Has the person's identity been verified? Do you need to verify the identity at this stage? If no, what event will trigger the need to verify the person's identity? Is this person a customer or a user? Was misleading marketing used to attract him or her? Have all the required notices and information been provided to the person? Is this person on the Office of Foreign Asset Control's (OFAC) prohibited list? What state is the person located in and what state level laws may apply?

From that small example, imagine the questions presented when a person funds the account and initiates a transaction. For each question, there is a governing law or regulation requiring compliance. And for each law, rule, or regulation every cryptocurrency exchange classified as a money transmitter by FinCEN needs to have a written policy.

Are you a money transmitter under FinCEN regulations?

Most cryptocurrency exchanges and DeFi apps will be MSBs because their business activities are those of a money transmitter. According to the general rule set out in FinCEN's 2019 guidance, a business is a money transmitter if its activities include:

- Exchanging virtual currency for real currency, funds, or other virtual currency; or
- Issuing a virtual currency and having the authority to redeem it; or
- Moving virtual currency or money from one location or account to another.

Decentralized exchanges and applications are not immune to FinCEN's oversight and rarely escape their money transmitter label. Unlike the Howey test for securities which examines the reliance upon a specific entity to increase value (centralization of control), it is the activities of the business that determine whether a cryptocurrency exchange is a money transmitter — a point illustrated by FinCEN's inclusion of analysis concluding that more often than not peer-to-peer (P2P) exchanges and decentralized applications (DApps) are money transmitters. Centralized or decentralized, so long as the activities are among those of a money transmitter the general rule is a cryptocurrency exchange or DApp will be a MSB subject to the BSA's AML requirement.

And as with any general rule, there are exceptions. Under FinCEN's latest guidance:

- Trading platforms that only matches buyers and sellers with the parties settling the transaction themselves are exempt. However, the exemption may disappear when the platform participates in the transaction — for example, participation in the completion of the trade.
- Some digital security offerings are exempt. With two (2) common exceptions being when:

- A person involved as an issuer, intermediary or investor is (1) a bank or a foreign bank, or (2) registered and functionally regulated or examined by the Commodities Future Trading Commission (CFTC) or Securities and Exchange Commission (SEC) or (3) a foreign financial agency that if in the United States would be required to register with the CFTC or SEC. However, these parties may be subject to other regulations imposing similar duties.

- The acceptance and transmission of value is fundamental to the sale of goods or services other than money transmission —an exception illustrated in FinCEN's 2008 guidance for brokers and dealers in currency and other commodities (and referenced again in 2019), stating that bona fide sales of currency or its substitute between a broker or dealer and a third party are exempt. Again, this exception only applies to FinCEN's money transmitter status and other regulations may apply.

- DApp development is exempt because the production of goods and services is not within the definition of a money transmitter. But a developer using or deploying the DApp for money transmission is treated as other DApp users and may be classified as money transmitters.

- Some wallets are exempt depending on if the wallet is within FinCEN's definition of a money transmitter which is based on four (4) criteria: (1) who owns the value; (2) where the value is stored; (3) the owner's direct interaction with the payment system; and (4) the intermediary's control over the value. On one end of the spectrum is hosted wallets where the host is a money transmitter. On the other end, the user-owner of a single-signature unhosted wallet is not a money transmitter if he has complete, independent control and interacts directly with the payment system to purchase goods or service's on his own behalf.

Don't be a Hero: Noncompliance may earn you a free vacation in a federal penitentiary!

Describing yourself as DeFi, decentralized or other similar terms does not shield you from legal requirements or repercussions. For starters, those are not legal terms — regulators and some judges may understand the meaning but no legal definition exists, yet. Under the current regulatory scheme, being sufficiently decentralized may provide an escape from some legal obligations. However, decentralization has no bearing on the BSA's AML requirement.

Again, the only question is whether the activities of the exchange or DApp are the activities of a money transmitter. And FinCEN specifically identified P2P-style exchanges and DApps as likely money transmitters who are subject to the BSA's AML requirement.

Disregard that obligation to develop and implement an effective, written AML policy at your own peril because the penalties are severe. And individuals may find themselves personally exposed to civil or criminal penalties — time in a federal prison is a real possibility.

- Herocoin owner, Kais Mohammad, faced up to 30 years in a federal penitentiary for running an illegal MSB. He was sentenced to 2 years prison after pleading guilty and, as part of the plea agreement, he also forfeited cash, cyptocurrency, and 17 bitcoin ATMs.

- Federal prosecutors indicted the chief executive and 3 co-owners of Bitmex (incorporated in Seychelles) on charges of violating the Bank Secrecy Act and conspiracy to violate the Bank Secrecy Act for their failure to establish and implement an effective AML program.

Developing a culture of compliance

The BSA's AML policy mandate is the cornerstone of compliance, but it is not the only policy a cryptocurrency exchange business needs. Vital to both legal compliance and risk management is a set of related policies to guide the business's actions in a range of scenarios and a compliance officer to implement them.

The role of the compliance officer is both a mandated component of a compliant AML policy and the foundation for the expected culture of compliance. In general, the compliance officer oversees the day-to-day implementation of company policies and models the level of compliance expected by the company. Whereas decision making and supervision responsibilities are written into many of the policies themselves, it is essential that she exemplify the expected compliance behavior because her attitude towards compliance will determine whether events or conditions receive a compliant reaction and are directed to the appropriate decision-makers. And fundamental to the compliance officer's success is a set of well-written policies addressing all compliance matters.

Understanding the basic components of a written policy

Despite the different subject matter, all written policies will contain most or all of the following components:

- A stated purpose or objective. This may be as simple as following a specific law or a detailed statement addressing the "why" and how it relates to compliance and/or risk management.
- Reference to the law being implemented or any laws being relied upon.
- Definitions the essential concepts are clearly defined. For example, a policy may define who is a "user" and who is a "customer".
- Identification of the person or persons responsible for implementation, oversight, and decision-making.

- Guidelines setting out the details of who does what when a specified event happens and how the response should be done.

- Change log detailing any revisions to the policy.

What types of policies does a cryptocurrency exchange need?

As mentioned at the start, legal compliance for cryptocurrency exchanges and DApps calls for multiple policies because more than one law governs the application or exchange's activities. In addition to a written AML policy, some of the additional policies could include:

- ***Vendor Due Diligence Policy*** specifying how due diligence will be conducted, by whom, the frequency of review, and how vendor risk will be assessed.

- ***Customer Complaint Policy*** detailing how customer complaints are handled and recorded.

- ***Suspicious Activities Report (SAR) Filing Procedure*** for when a SAR needs to be filed according to other policies. The events triggering a SAR may be detailed here or in other policies — for example, in an elder abuse or transaction monitoring policy.

- ***Transaction Monitoring Policy*** identifying how the company will identify suspicious transactions, investigate them, determine if a SAR is required and other corrective actions including the closing of accounts.

- ***Law Enforcement Request Policies*** specifying how the company responds and the person or department an employee should forward the request to.

- ***OFAC Policy*** explicitly stating the business's compliance with OFAC regulations and prohibitions regarding transactions with persons or entities on OFAC's sanction's list.

- ***Graham-Leach-Bliley (GLBA) Policy*** is basically a federal level privacy policy.

- ***Reg E Policy*** for complying with laws governing electronic fund transfers.

- ***Elder Abuse Policy*** for identifying and responding to conduct that qualifies as Elder Abuse including filing a SAR.

- ***Unfair, Deceptive, or Abusive Acts and Practices (UDAAP) Policy*** explicitly complying with federal and state laws prohibiting misleading, deceptive, unfair and abusive conduct.

- ***E-Sign Policy*** establishing the requirements and procedures for obtaining electronic signatures.

- ***Unclaimed Property Policy*** identifying what is unclaimed property, the procedures for locating the owner, and when the property is given to the state.

- ***Market Manipulation Policy*** to comply with Commission Future Trading Commission guidelines.

- ***Marketing Policy*** applying marketing restrictions including prohibitions under UDAAP or other laws to marketing by the business and by third parties.

- ***Disaster Recovery Policy*** setting out how the business prepares for a disaster and how it will respond. Not only is this essential for financial reasons, but it is also essential to ensure continued compliance with other laws.

- ***Data Retention Policy*** identifies the different categories of collected data and determines when the data can be destroyed. Although some policies will explicitly address data and document retention, this policy ensures appropriate retention of all data and documents.

As you can see, legal compliance is more than AML. By developing all the proper policies at the outset, your business can establish a culture of compliance and focus on the profit-generating activities.

Contacts

Dilendorf Law Firm, PLLC

E-mail: md@dilendorf.com

Phone: +1-212-457-9797

Address: Dilendorf Law Firm
4 World Trade Center Suite 2979
New York, NY 10006

Max Dilendorf

Partner

E-mail: md@dilendorf.com

@dilendorf_law