Financial Crime Compliance Primer

U.S. Crypto

cable

Cable is the leader in automated financial crime assurance.

Anything less than full, continuous monitoring of your financial crime controls leaves room for error with massive potential losses of money, time, and reputation.

So why manually test 100 accounts when you can automatically monitor 100%?

With Cable, you can rest easy with complete assurance that your financial crime controls are working effectively and let Cable surface any regulatory breaches, control failures or financial crime risks in real time. Automated assurance is the next evolution in financial crime compliance beyond screening softwares and CRMs, and fundamentally upgrades the standard for assurance processes – saving you money and time, reducing risk, and letting you scale compliantly and with confidence.

What are you missing without automated assurance?

For more information or to schedule a chat with our team, visit cable.tech.

Summary

- The crypto industry is perceived as posing elevated financial crime risks. Ignoring your financial crime compliance can inhibit growth and lead to fines, reputational damage, and scrutiny by regulators and partners.
- Crypto businesses can trigger financial crime requirements if they are U.S. money services businesses; you should carefully assess whether your business model triggers U.S. financial crime obligations.
- Managing your financial crime risks requires understanding key areas of risks identified by regulators and partners, as well as your own unique risks.
- You can better avoid financial crime breaches and violations by learning from previous civil enforcement actions and ensuring your controls are operating effectively.

Introduction

Recent statistics estimate that the amount of crime involving virtual assets almost doubled in 2021, amounting to $14 billion in illicit transaction activity or about 0.15% of total virtual asset transactions. This only accounts for the illicit activity able to be detected, and likely underestimates the true amount of financial crime involving virtual assets.

For regulators, law enforcement, and consumers, the perception of the crypto space as posing elevated financial crime risks persists, particularly as use of cryptocurrency becomes more mainstream. Even President Biden's recent Executive Order on Ensuring Responsible Development of Digital Assets, which was a notable expression of government support for innovation in the crypto space, made clear the significant illicit finance risks posed by the lack of effective financial crime controls for virtual assets.

Given these concerns about financial crime risks, if you work in a crypto business, it is essential that you become familiar with applicable financial crime obligations.

This primer will give you a foundational knowledge of U.S. financial crime compliance in the crypto context by addressing the following topics:

- Why does financial crime compliance matter?
- What are your financial crime obligations and what will others expect?
- What are particular areas of financial crime risk you should monitor?
- What are mistakes to avoid from previous enforcement actions?

One initial note on terminology – in this document, we use terms like "virtual currency," "digital assets," and "cryptocurrency" interchangeably, unless otherwise specified, which reflects the variable language you will find in different types of U.S. regulatory guidance for financial crime purposes.

Why does financial crime compliance matter?

The explosion in use of virtual assets and the accompanying rise of illicit financial activity involving virtual assets – along with the pseudonymous nature of virtual currency transactions, the near instantaneous ability to transfer virtual assets across borders, and the difficulty of tracking payments – has resulted in significantly increased regulatory and law enforcement focus on the financial crime risks of virtual assets. Cryptocurrency is frequently on the news because of some illicit financial activity, whether it be sanctions evasion, ransomware, romance scams, money laundering or one of many other forms of illicit activity.

As a result, if your firm is operating in the crypto industry, you are under the microscope from a financial crime compliance perspective as regulators seek to strengthen financial crime regulation for the crypto industry.

But even beyond regulatory concerns, there are four key reasons that financial crime compliance needs to be a central focus for you.

1. Scrutiny from Partners

First, you may receive just as much or more scrutiny about the extent of your financial crime risk management from partner banks or other financial institutions as you do from regulators. This is because your partners have their own obligations to ensure compliance with anti-financial crime requirements. If they determine that you pose unacceptable risks to them, you may be unable to enter into or continue your relationships.

2. Your Bottom Line

Second, financial crime compliance affects your bottom line. Our own analysis of fines given by U.S. and UK regulators found that nearly $2 billion worth were given in 2021. This included fines levied on well-established banks, such as Natwest, which was fined £265 million, and Capital One, which was fined $390 million, but it also included fines against crypto businesses, such as BitMEX, which was fined $100 million.

3. Reputational Damage

Third, your reputation is at stake with financial crime issues. Consumers rely significantly on word of mouth or mainstream news sources in making decisions about cryptocurrency, and your association with illicit activity may cause potential customers to hesitate in trusting or choosing you over other service providers.

4. Growth

Finally, amid the fierce competition for market share, you might be tempted to focus all of your attention on revenue-generating elements of your business and treat financial crime compliance as a check-the-box exercise and a cost center. But, as regulatory scrutiny and supervision of the crypto industry increases, turning a blind eye to your financial crime compliance will prevent the very growth you seek. Whether it's a partner bank that refuses to enter into a business relationship with you, customers that decide to go with an alternative platform, or a regulator that levies a fine, a lack of attention to financial crime compliance can undermine your business. Conversely, prudent forethought and investment in ensuring you appropriately address your obligations and risks as you scale will set up a strong foundation for your growth.

What are your financial crime obligations and what will others expect?

Now that you know why financial crime compliance matters, let's dive into what it entails.

KEY TERMS

What is the Bank Secrecy Act (BSA) and the Financial Crimes Enforcement Network (FinCEN)?

The BSA (as amended by the USA PATRIOT Act in 2001) is the foundational law of the U.S. anti-money laundering (**AML**) regime, and it requires certain financial institutions to implement and maintain financial crime compliance programs. FinCEN is the U.S. Treasury Department bureau that implements the BSA.

What is the Financial Action Task Force (FATF)?

The FATF is an international anti-money laundering standard-setting body, in which the U.S. is an active participant. The FATF is important in the crypto space as it issues key guidance driving the international push for greater financial crime regulation and supervision of the crypto industry, with the latest such guidance having been issued in October 2021.

What is a "virtual asset" and what is a "virtual asset service provider" (VASP)?

These are both defined terms used by the FATF (but not in U.S. laws or regulations) and, as a result, are terms you will see referenced in this space.

- A virtual asset is broadly defined as a "digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes," but does not include digital representations of fiat currencies, like e-money.

  U.S. guidance instead often uses terms such as cryptocurrency, digital assets, virtual currency or "convertible virtual currency" (**CVC**). The latter term is defined by FinCEN as a medium of exchange that operates like a currency and has an equivalent value in real currency or acts as a substitute for real currency, but does not have all the attributes of real currency, including legal tender status, and includes cryptocurrency like Bitcoin.

- A VASP is a person or entity engaged in the business of exchanging virtual assets for fiat or virtual assets, transferring, safekeeping or administration of virtual assets or instruments enabling control over virtual assets, or participating in and providing financial services related to an issuer's offer and/or sale of a virtual asset. This term is also not used consistently in the U.S.

Are you subject to financial crime compliance requirements?

To understand your financial crime obligations, you need to first know if you are one of the financial institution types subject to FinCEN's AML regulations. Most commonly, crypto businesses may be considered "money services businesses" or **MSBs** – these are defined by FinCEN to include persons doing business wholly or in substantial part within the U.S. as, among other specified capacities, a "money transmitter."

Alternatively, if a crypto firm is required to register as a broker-dealer with the Securities and Exchange Commission, or as a futures commissions merchant or introducing broker with the Commodity Futures Trading Commission, these types of financial institutions are also subject to FinCEN's AML regulations.

The critical question that most crypto firms need to consider is whether your crypto-related activities cause you to be an MSB.

How do you know if you are an MSB?

While this can be a very fact-specific question requiring expert advice and a close examination of your exact activities, the basic idea is as follows.

You will be an MSB if you are a money transmitter, which are persons or entities that are engaged in the transfer of funds or that provide "money transmission services."

FinCEN defines money transmission services broadly to include "the acceptance of currency, funds, or *other value that substitutes for currency* from one person and the transmission of currency, funds, or *other value that substitutes for currency* to another location or person by any means."

That expansive language in the money transmitter definition – "other value that substitutes for currency" – means that any transmission of virtual currencies will likely trigger MSB status, unless an exemption applies. While certain excepted activities don't lead to money transmitter status (e.g., certain types of payment processing, operating clearance and settlement networks, providing prepaid access, or transmitting funds "only integral to" your provision of goods or other services), these exceptions are very narrowly interpreted by FinCEN. You should expect FinCEN to take a broad view as to the types of crypto-related activities that trigger MSB status.

FinCEN provided further guidance in 2019, explaining that "users" that simply obtain virtual currencies to purchase goods and services on their own behalf are *not* money transmitters. On the other hand, "exchangers" – or persons in the business of exchanging virtual currencies for other real or virtual currencies – as well as "administrators" – or persons in the business of issuing and redeeming virtual currencies

– are generally money transmitters and thus considered MSBs. So, for example, you will find that crypto exchanges operating in the U.S., such as Coinbase and Kraken, are registered as MSBs with FinCEN.

There are a few other business models that FinCEN has indicated generally trigger MSB requirements in its 2019 guidance. These include, among others, peer-to-peer (**P2P**) exchangers, hosted wallet providers, crypto ATMs, decentralized applications (**DApps**) that perform money transmission or their owners/operators, mixers or tumblers, and crypto payment processors. Conversely, certain activities generally do not trigger MSB status according to FinCEN, such as solely mining virtual currencies or developing a DApp, without engaging further in money transmission.

It bears repeating that you should carefully assess if you may be an MSB and not assume financial crime obligations do not apply to you. Regulators are concerned that many crypto firms operating in the U.S. that do qualify as MSBs are not complying with their AML obligations.

If you're an MSB, what does this mean for your compliance obligations?

FinCEN imposes specific financial crime compliance requirements on MSBs. At a high-level, you will be required to:

1. Compliance Program
Implement an AML compliance program consisting of 5 main "pillars" -

- Policies, procedures and internal controls reasonably designed to assure your compliance with financial crime regulations;
- A designated compliance officer;
- Employee training;
- Independent testing to evaluate the effectiveness of your compliance program; and
- Risk-based procedures for ongoing customer due diligence to understand the nature and purpose of customer relationships.

As an MSB, you will be examined by the Internal Revenue Service (**IRS**) for compliance against these 5 pillars.

2. Suspicious Activity Reports
Make "suspicious activity reports" (**SARs**) to FinCEN for any unusual or suspicious transactions you detect, as well as currency transaction reports for cash transactions over a threshold amount.

3. Register
Register with FinCEN as an MSB and obtain all required state money transmitter licenses where you are engaged in money transmission activities.

Failing to comply with your state licensure or federal MSB registration requirements may result in a monetary fine. You could also face federal criminal penalties for operating an unlicensed money transmitting business.

What will your banking partners require from you?

In reality, you may find that the greatest scrutiny of your financial crime compliance program comes from your banking partners, and not from regulators. In fact, the U.S. Treasury Department reported that the IRS examiner force is only half the size it was in 2010 and faces the challenge of examining increasingly complicated crypto business models and rising numbers of MSBs.

While banks are not expected or supposed to be a *de facto* regulator of MSB customers, your partner banks must still take a risk-based approach to managing potential financial crime risks that you may pose to them.

You must be able to assure yourself and your partners that you are appropriately managing your financial crime risks through effective controls.

Banks likely will request you to confirm your FinCEN registration as an MSB and your compliance with applicable state licensing requirements. They may also request a host of other due diligence measures from you. These may range from diligence questions about your financial crime policies, procedures, and controls, such as information on recent regulatory breaches or control failures, to contractual requirements obligating you to provide representations about the design and effectiveness of your AML compliance program, the nature of your business, anticipated activity, products and services, or geographies and markets you serve.

If a bank determines you present higher financial crime risks, they can require further enhanced diligence measures of you in order to be comfortable proceeding with the relationship. In practice, banks have differing risk appetites for crypto customers, which may depend on your particular business model, their familiarity with crypto businesses, and their perception and understanding of the financial crime risks you pose.

What other financial crime requirements should you keep top of mind?

In addition to the basic financial crime compliance obligations touched on above, you should be aware of certain other requirements that are currently regulatory priorities.

Travel Rule Obligations
One of the key AML requirements for financial institutions is the so-called “Travel Rule,” which requires certain information about the parties to a transaction to “travel” with the transaction to the receiving entity. You may hear the Travel Rule also referred to as FATF’s “Recommendation 16,” which is where this requirement can be found in FATF’s

AML standards.

In 2019 guidance, FATF said the Travel Rule should apply to virtual asset transfers above $1,000 between VASPs or a VASP and another financial institution. Subsequently, in 2020, FinCEN proposed controversial and still-pending rules to unambiguously extend the U.S. Travel Rule to virtual currency transactions.

The Travel Rule is a regulatory priority as it enables records to be retained on transactions for law enforcement or national security purposes. However, the difficulty with the Travel Rule is in finding real-world technical solutions for actually complying with the information required to be collected about beneficiaries for virtual currency transactions. The FATF did recognize this challenge, noting in 2019 that it wasn't aware of "technically proven means" that would enable the Travel Rule requirements to be met in all cases.

Nonetheless, this has not stopped other jurisdictions from seeking to extend Travel Rule obligations to virtual currency transactions, including the EU, which recently voted to move forward with a proposal to apply Travel Rule obligations to all virtual currency transactions without a de minimis threshold. As a result, the crypto industry is actively seeking different solutions to enable compliance with Travel Rule obligations given the broad momentum in this direction.

Unhosted Wallets
Similarly, in 2020, FinCEN also proposed still-pending rules that would require MSBs to comply with a range of recordkeeping, identification and verification requirements for virtual currency transactions that involve unhosted wallets or wallets in certain high-risk jurisdictions. Again, the technical compliance burden would be difficult, but other jurisdictions around the world are also contemplating similar rules for unhosted wallets.

Sanctions
Finally, the U.S. maintains economic sanctions prohibiting all U.S. persons from engaging in dealings with sanctioned persons and jurisdictions. These are distinct obligations that apply to any U.S. person or entity, or anyone located in the U.S., and therefore do not depend on your MSB status. In 2021, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC), which administers and enforces U.S. sanctions, issued seminal guidance for the virtual currency industry, which made clear that virtual currency transactions are equally subject to U.S. sanctions compliance obligations.

It is critical that you implement and maintain an appropriately scaled sanctions compliance program to ensure you do not violate U.S. sanctions, particularly as the U.S. increases its use of sanctions as a foreign policy and national security tool.

What are particular areas of financial crime risk you should monitor?

Now that you have a basic understanding of your financial crime risk management and compliance obligations, the natural next question is...what does this mean in practice?

In other words, what kind of financial crime risks are you expected to identify and manage? Unfortunately, there is no one-size-fits-all answer. Your risks depend on the nature of your business and the activities you engage in, and you need to assess the unique risks you face in order to properly manage them.

However, there are practical steps you should take to understand your risks. In particular, you should be aware of the most pressing financial crime risks posed by cryptocurrencies that have been identified by regulators and law enforcement. Must-read guidance about red flags for illicit activity involving virtual currencies was published by FinCEN in 2019. Additionally, you may find helpful the recent reports on crypto crime trends and typologies published by Chainalysis and Elliptic, two of the leading blockchain analytics companies.

Below, we give you an overview of the significant areas of financial crime risk related to virtual currencies.

You must understand and manage key areas of financial crime risks identified by regulators and partners, as well as your own unique financial crime risks.

Ransomware

In the wake of several notable ransomware attacks in 2021 against U.S. infrastructure providers, FinCEN issued updated guidance on financial crime risks posed by cyber ransom attacks. In the first half of 2021 alone, FinCEN estimated that there was nearly $600 million worth of ransomware-related suspicious activity. The financial crime risks arise from the fact that virtual currencies are ransomware perpetrators' preferred form of payment, via virtual currency exchanges that often have weak or no AML controls and a variety of virtual currency laundering methods, such as the use of mixers, tumblers, or chain hopping techniques.

You should expect financial institutions to be wary of any potential ransomware connections or risks you may have, given the heightened regulatory and law enforcement sensitivity to these issues and the potential civil and criminal liability for any parties involved in a ransomware transaction.

Sanctions evasion

The expansive sanctions recently imposed on Russia brought back to light U.S. authorities' concern that sanctioned parties may evade U.S. sanctions using virtual currency. Other sanctioned jurisdictions, like Iran, North Korea, and Venezuela, have turned to virtual currencies to get around U.S. sanctions. Red flags for potential Russian sanctions evasion attempts, such as virtual currency transactions initiated from IP addresses in Russia, Belarus, or other high-risk or sanctioned jurisdictions, are provided in recent FinCEN guidance, and it's more important than ever that you take steps to ensure your sanctions controls are operating effectively.

That said, prominent U.S. government officials have said there are no signs of significant Russian sanctions evasion through cryptocurrency yet, in part because of the application of AML obligations to crypto exchanges. Nevertheless, the perception that cryptocurrency may facilitate sanctions evasion attempts has certainly increased regulatory and law enforcement scrutiny of cryptocurrency activities. For example, the U.S. recently sanctioned a Russian virtual currency mining company in order to ensure that "no asset, no matter how complex, becomes a mechanism for the Putin regime to offset the impact of sanctions."

Certain crypto business models

Crypto businesses are not all the same, and the inherent financial crime risks vary depending on the particular customers, products, and services of various business models. U.S. regulators have emphasized that some types of crypto businesses pose greater financial crime risks than others. Higher-risk businesses include crypto ATMs, some of which avoid their U.S. AML obligations intentionally in order to attract criminals seeking to engage in illicit activities using cryptocurrencies. Other business models posing elevated risks include unregistered P2P exchangers or foreign-located MSBs operating in the U.S., which may similarly intentionally avoid AML obligations or offer services to anonymize or conceal transactions, and therefore also gain popularity amongst criminals seeking to transact in cryptocurrency.

Decentralized Finance (DeFi)

DeFi describes the use of blockchains to provide financial services without the involvement of a centralized party. Research has estimated the amount of money laundering through DeFi protocols increased to nearly $900 million in 2021, amounting to a 1,964% increase compared to 2020. The surge in money laundering through DeFi protocols may be a result of illicit actors' attempts to find other ways to transact outside of centralized exchanges that are more likely to have AML controls. Given their decentralized nature, DeFi services are less likely to have AML controls or other preventive measures against money laundering or illicit transactions.

Anonymity-Enhanced Cryptocurrencies (AECs)

AECs are types of cryptocurrencies designed to anonymize or obfuscate virtual currency transactions by using private blockchains. Given the difficulty in tracing transactions using AECs and the lack of transparency into the details of such transactions, AECs pose elevated risks of being used by illicit actors seeking to conceal or disguise their criminal dealings. For example, FinCEN indicates ransomware perpetrators often demand payment in the AEC, Monero, which has become closely associated with illicit activity in the eyes of regulators.

Darknet marketplaces

A wide variety of illicit activity is associated with darknet marketplaces, including drug and arms trafficking, fraud, and cybercrime. Virtual currencies are often the preferred or only method of payment on such marketplaces. As a result, any nexus with darknet marketplaces will raise concerns about potential illicit activity for financial institutions. The U.S. recently sanctioned and helped to shut down Russia-based Hydra Market, the world's largest darknet marketplace, which was estimated to be responsible for 80% of all darknet market-related cryptocurrency transactions in 2021.

Fraud

Virtual currencies have also been implicated in a variety of fraudulent schemes, such as impostor scams targeting the elderly or unemployed, investment scams, scams using hacked Twitter accounts of celebrities and companies, and romance scams (which resulted in $139 million of losses in cryptocurrency in 2021 alone, or nearly a five times increase compared to 2020).

What are mistakes to avoid from previous enforcement actions?

Finally, it's always helpful to learn from others' mistakes. Below, we summarize key enforcement actions involving previous instances in which crypto firms have failed to meet their financial crime obligations.

Given the more recent emergence of virtual currencies, the number of past civil enforcement actions is relatively low. However, with the increased regulatory focus on financial crime risks in the crypto space, you should expect heightened enforcement activity by U.S. authorities regarding crypto firms' financial crime controls.

AML breaches

- In 2015, FinCEN brought its first enforcement action against a virtual currency exchanger, with a $700,000 fine against Ripple Labs for failing to register with FinCEN as an MSB, establish an AML compliance program, or file SARs with FinCEN, even though it sold virtual currency and was therefore an MSB. This case demonstrates the reality that if you have financial crime issues, beyond the monetary impact of potential fines, you also may face a slew of increased compliance burdens that impede your capacity to focus on growth or expansion activities. Ripple's required remedial steps were extensive, including a multi-year "look-back" exercise to identify prior suspicious transactions, a requirement for external auditors to review the firm's BSA compliance through the next five years, and required enhancements to the Ripple Protocol to enable appropriate monitoring of transactions.

- FinCEN expanded its reach in 2017 with its first enforcement action, and a much more sizeable fine of $110 million, against a foreign-located virtual currency exchanger, BTC-e, which conducted transactions for U.S. persons and thus triggered U.S. AML obligations. This action exemplifies the significant financial crime risks posed by non-U.S. virtual currency exchanges that do not abide by AML controls and market themselves to illicit actors. Specifically, BTC-e facilitated numerous transactions involving ransomware, cybercrime, fraud and identity theft, corruption, and drug trafficking, and even advised users how to transfer funds from illicit sales on darknet marketplaces. The U.S. Department of Justice (**DOJ**) also indicted the exchange and its operator on criminal charges.

- In 2019 and 2020, FinCEN once again expanded its enforcement scope by bringing its first enforcement actions against an individual operating as a P2P exchanger and another individual operating two mixers. In both instances, the regulatory breach was operating as unregistered MSBs and failing to implement an AML compliance program or file SARs. In the latter case, similar to the case of BTC-e, the operator of the mixers deliberately avoided AML obligations, actively aided criminals in evading AML controls at virtual currency exchanges and engaged in a wide range of transactions with illicit actors, also leading to his criminal prosecution by DOJ.

- Finally, in 2021, FinCEN imposed a $100 million fine on BitMEX, one of the oldest and largest foreign-located virtual currency derivatives exchanges, again for failing to maintain an AML compliance program or file SARs with FinCEN. BitMEX was engaged in money transmission services, but was obligated primarily as a futures commission merchant operating in the U.S. to comply with BSA requirements. FinCEN discovered that the exchange attracted illicit actors due to its lack of customer due diligence requirements, leading it to engage in numerous transactions with darknet marketplaces, scammers, sanctioned individuals, and unregistered mixing platforms offering money laundering services. As part of its required remediation efforts, BitMEX had to conduct a lookback over a six-year period for suspicious transactions, as well as engage an independent consultant to review its controls for ensuring it does not conduct business in the U.S.

Sanctions violations

In 2020 and 2021, OFAC brought its first sanctions enforcement actions against crypto firms, including the virtual currency payment processor, BitPay, and the digital asset service provider, BitGo. In both cases, the firms failed to screen available location data in their systems about persons using their platform or services that were located in sanctioned jurisdictions at the time, such as Crimea, North Korea, Cuba, Iran, Sudan and Syria.

These examples demonstrate the importance of not only making sure you have controls in place to comply with your financial crime obligations, but ensuring you have the means of assuring yourself those controls are working as intended or finding gaps that need to be fixed.

Conclusion

The financial crime landscape has become more fraught due to novel technologies, different types of bad actors, and new types of illicit financial schemes – and the crypto industry ticks all of these boxes. Financial crime is a primary focus of U.S. authorities and you ignore your compliance obligations and expectations at your own peril.

It is critical, no matter your stage of growth, to ensure you have an appropriately scaled compliance program to avoid financial crime breaches, failures, and risks. You need a means of assuring yourself that you have set up controls that are effectively operating at all times, and you also need to be able to demonstrate this fact to others that will expect the same. Doing so will give you a strong foundation upon which you can scale with confidence. This is all possible with the right investment and attention, and with this primer, you now have foundational knowledge that hopefully helps you and your financial crime team take the next step forward!

cable

cable.tech