The Guide
to Anti-Money Laundering - First Edition

AML Compliance for Cryptocurrency and other Virtual Assets
The Guide to Anti-Money Laundering - First Edition

The Guide to Anti-Money Laundering is one of the first volumes to tackle both sides of the money laundering conundrum simultaneously. It covers enforcement trends around the world in Part I and compliance trends in Part II – with specific practical advice for corporations and their counsel throughout. It is an addition to GIR’s technical library – made famous by The Practitioner’s Guide to Global Investigations – that now includes guides to, among other things, monitorships, compliance and sanctions.
AML Compliance for Cryptocurrency and other Virtual Assets

Stella Mendes, Andrew Rosini, Jaco Sadie and Keenan Mahoney
FTI Consulting

Summary

- COMPLIANCE ACTIVITIES’ CHALLENGES AND SOLUTIONS
- ONBOARDING AND KNOW-YOUR-CUSTOMER PROGRAMMES
- TRANSACTION MONITORING
- BENEFICIAL OWNERSHIP AND DIRECT/INDIRECT EXPOSURE
- HOW REGULATORY ENVIRONMENT IS EVOLVING ON CRYPTO AND VIRTUAL ASSETS
- STEPS FOR COMPLIANCE TEAMS TO TAKE
- ENDNOTES
Compliance with anti-money laundering (AML) and counter-terrorist financing (CFT) is becoming more complex as the global financial system – and the regulatory environment that governs it – continues to evolve. AML compliance professionals find themselves focusing their battles on two fronts: traditional finance (TradFi) and decentralised finance (DeFi), with a diverse and growing set of virtual assets that can be held, transferred or traded. Compliance is particularly challenging at the intersection of these two fronts, involving fiat currency and cryptocurrency.

As Paul Grewal of Coinbase, the largest crypto exchange in the United States, wrote in a June 2023 blog: 'With more than 20 percent of Americans owning and using crypto, we need a regulatory framework that will protect consumers and enable the critical uses of this new technology to continue and grow.'

The number of distinct cryptocurrencies and digital assets continues to increase. Since the 2008 launch of Bitcoin, which remains the best-known cryptocurrency as well as the largest by market capitalisation, thousands of digital currencies have been coined. Virtual assets is a term that describes a wide range of digital objects, including cryptocurrency, stablecoins pegged to a reserve currency such as the US dollar, non-fungible tokens (NFT) and security tokens that resemble tradable stocks and bonds. A new form of virtual asset that has emerged in the past few years is DeFi tokens, which can mimic traditional financial system products such as loans and savings accounts.

From an AML compliance standpoint, regulatory requirements for virtual assets are essentially the same for fiat currency and tangible assets. The most important aspect of all AML compliance programmes is that they should be designed to prevent criminals from using the global financial system to launder their ill-gotten gains, whether those are in fiat currency or cryptocurrency. Financial institutions’ AML compliance teams, therefore, must meet the same standards regardless of the type of asset. If a traditional financial institution opts to serve its customers using digital assets, the institution cannot apply a different standard of compliance, even if the tools used for transaction monitoring and other activities differ for virtual assets. As Adrienne A Harris, superintendent of the New York State Department of Financial Services, has explained: ‘All virtual currency companies licensed in New York State are subject to the same anti-money laundering, consumer protection, and cybersecurity regulations as traditional financial services companies.’

Internationally, regulatory jurisdictions are implementing or considering rules for cryptocurrency and other virtual assets. For example, although cryptocurrency has been fully legalised in 20 countries analysed by the Atlantic Council – including the United States, Canada, the United Kingdom, Australia, Germany, Japan and Singapore – only 14 currently have AML/CFT regulations that apply to cryptocurrency. As with any emerging technology, the pace of regulation has not kept up with the pace of adoption, and the disparate rules in various jurisdictions add to the challenge with compliance for institutions with global operations.

In the 45 countries the Atlantic Council studied, entities regulated for cryptocurrency and virtual assets include crypto exchanges, crypto issuers, traditional financial institutions, cryptoasset service providers and cryptocurrency miners. The regulatory status the council assigned to each of these jurisdictions are (1) legal, meaning all activities are permitted, (2) partial ban, or some activities are not permitted, and (3) general ban, signifying that all crypto and virtual asset activities are not permitted.
Ten of the G20 countries have legalised crypto and virtual assets, representing 50 per cent of global gross domestic product. [8] According to the Atlantic Council, all members of the G20 are considering crypto regulations. An emerging area of virtual assets is stablecoins, which are usually backed by a fiat currency (except for algorithmic stablecoins that are unbacked by fiat currency). Regulation of stablecoins is under consideration in the European Union, the United Kingdom, the United States and Thailand. Among G20 countries, Mexico has a partial ban on crypto and virtual assets, and currently does not permit financial institutions to issue stablecoins. [9]

In October 2021, the Financial Action Task Force (FATF) updated its guidance for a risk-based approach to virtual assets and virtual asset service providers (VASPs). The FATF noted that its recommendations apply to virtual assets and VASPs in the same way as they do to traditional financial institutions. The FATF is not attempting to regulate either the users of virtual assets or the technologies on which virtual assets are traded or used to conduct trades or transfers. Rather, the FATF is trying to clarify definitions of virtual assets and VASPs and provide guidance on the risks and tools to address money laundering and terrorist financing risks in peer-to-peer transactions. [10]

What is changing steadily about virtual assets are their types, utilisation by individuals and corporate entities, and their value. Although this is a challenge for compliance professionals to stay current on the dynamic marketplace for virtual assets, an even bigger challenge may be what is not changing: regulatory expectations for AML compliance.

**COMPLIANCE ACTIVITIES’ CHALLENGES AND SOLUTIONS**

Arrayed against compliance professionals’ efforts to combat money laundering and terrorist financing are criminal entities that have proven themselves to be highly adaptable. From rogue actors to organised and state-sponsored enterprises, the opponents are adept at exploiting loopholes and altering tactics to maintain their flows of illicit funds. Virtual assets have become a popular mode of transferring and storing value, in part because there is a perception that they enable counterparties to remain anonymous in transactions. For obvious reasons, this benefits those with criminal intent; but anonymity in virtual assets has its limits – in fact, virtual assets are considered pseudo-anonymous.

Individuals familiar with the basic workings of cryptocurrency may assume all virtual asset transactions are recorded on distributed ledgers known as blockchains. Just as the internet encompasses both public and private cloud servers, the crypto world also has public and private blockchains. Although many cryptocurrency transactions are indeed recorded on public blockchains, many are not, especially those that take place on centralised exchanges. ‘Off-chain’ transactions, although less secure, nevertheless can provide faster service and lower fees than those that occur ‘on-chain’, such as Bitcoin’s public blockchain.

On-chain transactions are immutable and traceable, as digital wallets have public addresses and movements of funds are viewable on blockchains. Once a crypto transaction is verified on a blockchain, a record of it is stored on all ledgers on that chain. This fact is good news for AML/CFT compliance, as it enables analysis and attribution to wallet holders using sophisticated tools. The downside, and why virtual assets are pseudo-anonymous, is that each party in a transaction retains a secret key. The public address of a digital wallet remains visible but not the name of the user associated with that wallet. A significant challenge exists for compliance professionals in discerning the names to which digital wallets are attributed.
Fortunately, compliance teams can enlist assistance in that effort from technology-enabled expert services.

The scale of crime involving digital wallets and movement of virtual assets, relative to all cryptocurrency volume, is minuscule: in 2022, the amount of crypto activity associated with illicit activities was 0.24 per cent, up from 0.12 per cent in 2021, according to blockchain data analysis company Chainalysis.\[11\] The value of crime in cryptocurrency, however, is quite large. In its 2023 Crypto Crime Report, Chainalysis reports that cryptocurrency values received by illicit addresses hit an all-time high of US$20.6 billion in 2022, up from US$18.1 billion in 2021. The three predominant sources of illicit revenues in 2022 were sanctioned entities, scams and stolen funds. Chainalysis notes that these figures do not include non-crypto crimes, such as conventional drug trafficking, that use cryptocurrency as payment.\[12\]

**ONBOARDING AND KNOW-YOUR-CUSTOMER PROGRAMMES**

The pseudo-anonymous nature of virtual assets is a hurdle that compliance teams must clear to fulfil their mission to prevent or disrupt criminal use of the financial system. With the value of illicit activity rising in cryptocurrency, the stakes are getting higher.

Conducting know-your-customer (KYC) and customer due diligence (CDD) activities in an online environment poses a different kind of challenge from how onboarding has been done traditionally; for example, many more kinds of customers are coming to financial institutions through online channels, rather than face-to-face. The emergence and proliferation of financial technology companies (fintechs) have accelerated financial institutions’ adoption of digital onboarding. Fintechs have pushed banks to expand their onboarding from manual, paper-based processes and human identification verification to fully digital and automated verification using biometrics and, very often, third-party databases. Onboarding and KYC for customers with virtual assets requires a similar digital approach, while managing AML risks. The FATF guidance notes that virtual assets:

> enable non-face-to-face business relationships . . . . Further, [virtual assets] can be used to quickly move funds globally . . . and to facilitate a range of financial activities—from money or value transfer services to securities, commodities or derivatives-related activity, among others. These factors in [virtual asset] financial activities or operations may indicate higher ML/TF [money laundering/terrorism financing] risks.\[13\]

A critical component of onboarding and KYC is wallet screening. When conducted during onboarding and for ongoing KYC, wallet screening and due diligence help to identify bad actors by recognising risk exposure and, in some instances, associating wallets with a known entity or individual. Transactions outside the financial institution’s risk threshold can be blocked and fraud can be combated by pinpointing a wallet’s source and destination of funds. In turn, robust wallet screening provides users with confidence in executing trustworthy transactions and making links with other crypto wallets on the network, as well as helping to detect if a specific crypto exchange, sanctioned entity or darknet market is in control of a wallet.

For these reasons, compliance teams at TradFi institutions may find it useful to emulate the compliance steps that fintechs need to perform in the online environment in which
they operate. These include onboarding, risk rating, transaction review, identification of counterparties and periodic reviews.

Onboarding customers to open accounts requires careful and consistent processes that may involve seeking additional information to establish and verify a customer’s identity, including obtaining documentation verifying complex ownership structures and the identities of any beneficial owners. KYC and CDD are merely the first steps in the AML compliance journey. A risk-based compliance programme enables institutions to allocate resources to more effectively align with their AML risks.

TRANSACTION MONITORING

Transaction monitoring is another key component in compliance programmes that lets financial institutions spot trouble and take action. An effective transaction monitoring programme establishes a feedback loop between an institution’s KYC and customer risk rating activities. Risk-based compliance requires monitoring and maintaining an up-to-date risk rating, as customers’ financial behaviours can and do change.

Compliance teams should continuously analyse customers’ transactions involving such assets in the context of cryptocurrency and other virtual assets; for example, a customer may convert fiat currency into cryptocurrency and vice versa. Similarly, institutions should monitor the outbound and inbound movement of crypto assets recorded on-chain and the movements of crypto assets off-chain, paying particular attention to unusual transaction patterns or transactions involving high-risk customers and locations.

A component of transaction monitoring is know your transaction (KYT), which is a process that financial institutions use to monitor, track and evaluate financial transactions to detect and prevent fraudulent or criminal activity. As cryptocurrency use grows, institutions must understand how crypto transactions carry bits of information with them so compliance teams can investigate these transactions for evidence of financial crimes. Additionally, KYT allows financial institutions to comply with AML regulations and protect their reputations and customers from financial crime. Without KYT, financial institutions would be at risk of unknowingly facilitating illegal activity, which could lead to legal penalties, financial losses and reputational damage.

KYT clarifies whether a person or business engages in illegal financial activity. It is a critical tool for financial institutions to ensure compliance with regulations, prevent financial crime, protect their customers and reputation, and analyse financial behaviour for oddities in individual transactions and patterns across multiple money moves. Together with KYC, financial institutions can supplement a well-established KYC/CDD process with additional steps when they offer a virtual asset product or service.

TradFi institutions typically get into crypto by offering it to existing customers. When establishing the expected activity of a customer, in addition to the usual questions about cash and wire transfers, the institution may ask if the customer plans to engage in cryptocurrency transactions. That could lead to follow-up questions: What kinds of coins/tokens? What are the customer’s current wallet addresses? From what wallets will the customer send funds to the institution? Will the customer engage in DeFi, or peer-to-peer, transactions? The KYC process can allow compliance teams to determine whether the expected activity of the customer is legal in their jurisdiction, and then allow the institution to screen existing wallets for direct and indirect exposure to unusual activity. Institutions can then design transaction monitoring alerts when customers send in funds through
undisclosed wallets. The results of transaction monitoring help to create configurable wallet risk scoring so that users can better understand their transaction counterparties. That is why wallet screening, KYT and transaction monitoring remain integral parts of an adequate AML programme.

**BENEFICIAL OWNERSHIP AND DIRECT/INDIRECT EXPOSURE**

To meet AML compliance requirements, institutions must gather information about counterparties to determine whether the movement of funds is suspicious. Even though crypto wallet addresses and the movement of funds are visible in virtual asset transactions on public blockchains, attribution of these addresses often requires additional analytical tools. For example, virtual asset monitoring companies have attributed wallet addresses to criminal and high-risk entities, including those that are subject to sanctions.

Institutions handling virtual assets can have direct exposure to the counterparties in a blockchain transaction as well as indirect exposure; that is, institutions face exposure to other addresses with which the counterparty has transacted. Indirect exposure can occur in both the sending and receipt of funds, and where they originate as well as their destination. Asset tracing takes on even more importance when those assets are virtual, but the good news for compliance teams is that tracing is easier thanks to the transparency of the distributed ledger system in blockchains.

In contrast, indirect exposure does not exist for institutions handling cash. It is not possible to track fiat currency in a centralised place to determine whether or where it has been in the hands of criminals. Except when cryptocurrency enters centralised crypto exchanges, mixers or tumblers, indirect exposure in crypto can be measured to a degree. Just as criminals using traditional financial institutions attempt to obfuscate and obscure the origin of their illicit funds by shifting them through a series of entities and other financial institutions, a similar technique exists in cryptocurrency. A cryptocurrency holder may possess multiple wallets to collect and transfer funds to intermediary non-service addresses on their way to a service address, such as a crypto exchange, through what are known as ‘hops’.

Transaction monitoring for virtual assets, therefore, should take into account direct and indirect exposure and create alerts to prompt further investigation. Examples of alerts that could uncover suspicious activity include those for multiple hops, as well as *ex post facto* receipt of virtual assets. Cryptocurrency exchanges cannot prevent the inflow of virtual assets but they can screen transactions after the fact to determine whether the target destination is associated with illicit addresses. Aligning transaction monitoring and alerts to guidance on trends and criminal typologies provided by the Financial Crimes Enforcement Network (FinCEN) also is a prudent step.

As the FATF notes:

> [virtual asset] products or services that facilitate pseudonymous or anonymity-enhanced transactions also pose higher ML/TF risks, particularly if they inhibit a VASP’s ability to identify the beneficiary. Lack of customer and counterparty identification is especially concerning in the context of [virtual assets], which are cross-border in nature. If customer identification and verification measures do not adequately address the risks associated with non-face-to-face or opaque transactions, the ML/TF risks increase, as
does the difficulty in tracing the associated funds and identifying transaction counterparties.\[14\]

**HOW REGULATORY ENVIRONMENT IS EVOLVING ON CRYPTO AND VIRTUAL ASSETS**

The regulatory environment on cryptocurrency and other virtual assets is becoming more complex, like the objects of regulation themselves. Even though financial services regulators hold institutions to the same standards, whether they handle digital or fiat currencies, regulators do recognise that the domain of virtual assets is developing rapidly. As a result, regulations on digital currencies and virtual assets are multi-part. Compliance teams have to wrestle with requirements relating to cryptocurrency itself, the Bank Secrecy Act (BSA), anti-money laundering and cybersecurity.

Adding to the complexity is the reality that multiple regulatory authorities exercise jurisdiction over crypto and virtual assets. Within the United States, several federal agencies, as well as state regulatory authorities, issue rules regarding virtual assets; among those agencies are the Securities and Exchange Commission, the Commodity Futures Trading Commission and the US Department of the Treasury. Outside the United States, differing regulatory regimes make it difficult for compliance teams to establish and maintain a global approach to AML on crypto and virtual assets.

In April 2023, the European Parliament passed its Regulation on Markets in Crypto-Assets (MiCA).\[15\] The Regulation directs cryptoasset service providers to take steps to protect consumers and improve governance, and expands the entities that are subject to European AML rules. A separate, companion piece of legislation on AML is working its way through the European Parliament. This is intended to align the European Union AML approach with FATF standards on transfers of funds.

Regulation of the transfer of funds (TFR), also known as the Travel Rule, has long been a standard in fiat currency and is now being applied to cryptocurrency transactions. The Travel Rule sets a threshold at which institutions must identify the originators and beneficiaries of transactions. Jurisdictions differ on this, with the United States using a US$3,000 threshold for cryptocurrency transactions. The FATF initially suggested a threshold of US$1,000 or €1,000 for crypto currency transactions but new EU rules impose a €0 threshold, meaning all cryptocurrency transactions, regardless of size, must identify the originators and beneficiaries.\[16\]

In spring 2023, more jurisdictions announced plans to enforce AML regulations for cryptocurrency transactions. Japan announced plans to enforce strict AML rules, beginning in June, intended to bring the nation in line with global cryptocurrency regulations, including the Travel Rule. Japan’s application of this rule imposes a US$3,000 threshold on cryptocurrency transactions.\[17\] Similar action was taken in May 2023 by the United Arab Emirates, which indicated it would require licensed financial institutions to verify the identities of all customers, based on FATF standards, including relationships with virtual asset service providers, such as cryptocurrency exchanges.\[18\]

Regulatory actions by other jurisdictions on virtual assets are likely as more financial services regulators consider global standards. An FATF report showed that 75 per cent of jurisdictions are partially or fully non-compliant with virtual asset AML standards. The report cited a general lack of understanding of cryptocurrency markets, as well as compliance tools that are limited in scope or not interoperable to meet FATF standards.\[19\]
For compliance professionals, there is both a benefit and a challenge in the promulgation of regulations. The more national and other regulators that issue requirements on cryptocurrency and other virtual assets, the more legitimised these transactions become. More regulation, therefore, is likely to promote further use of digital assets, meaning financial institutions will see increasing volumes, and the AML compliance team’s workload will rise commensurately.

STEPS FOR COMPLIANCE TEAMS TO TAKE

The road ahead in AML compliance for cryptocurrency and other virtual assets may appear difficult to navigate, but financial institutions can chart a course to make the journey easier. A foundational step is to assess the existing five pillars of the BSA/AML compliance programme. These pillars must support an institution’s compliance efforts when it comes to fiat currency as well as cryptocurrency. Successful compliance programmes are built on:

- **Internal policies, procedures, and controls**: Monitoring and screening methodologies should be reviewed and updated as risk profiles change for a given institution. AML compliance teams’ controls – including algorithms for identifying and investigating suspicious activities, filing suspicious activity reports and conducting forensic reviews – are the true test. Without effective controls, institutions can veer off into compliance failures.

- **Designation of an AML officer**: Accountability is critical in compliance, and the designation of an AML officer, with the right balance of experience between compliance and virtual assets, is an important foundational step.

- **Employee training**: Keeping up with changes in regulations and jurisdictional differences is difficult enough. Add in marketplace changes and new forms of virtual assets and that task becomes vastly more complicated. Continuing employee training is recommended for all financial institutions.

- **Independent testing**: To be consistently effective, compliance activities and procedures should be properly designed, analysed and validated. An independent third party who is knowledgeable about AML and virtual assets can be a valuable partner in this effort.

- **Customer due diligence**: KYC and CDD are essential elements in AML compliance. Compliance programmes need to account for the risk factors that pertain to the specific institution. Risk scoring of existing and prospective counterparties is a critical step, for any asset type.

Another important step is to utilise trusted partners to assist in designing, validating or performing the critical services relating to AML compliance. These include KYC, CDD, blockchain analytics, transaction monitoring, sanctions screening and risk scoring.

Finally, specific and regular training for compliance teams on cryptocurrency and other virtual assets is recommended. Keeping up to date with new asset types, marketplace trends, typologies in the use of cryptoassets for money laundering and corresponding regulations is vital for effective AML compliance.

Endnotes