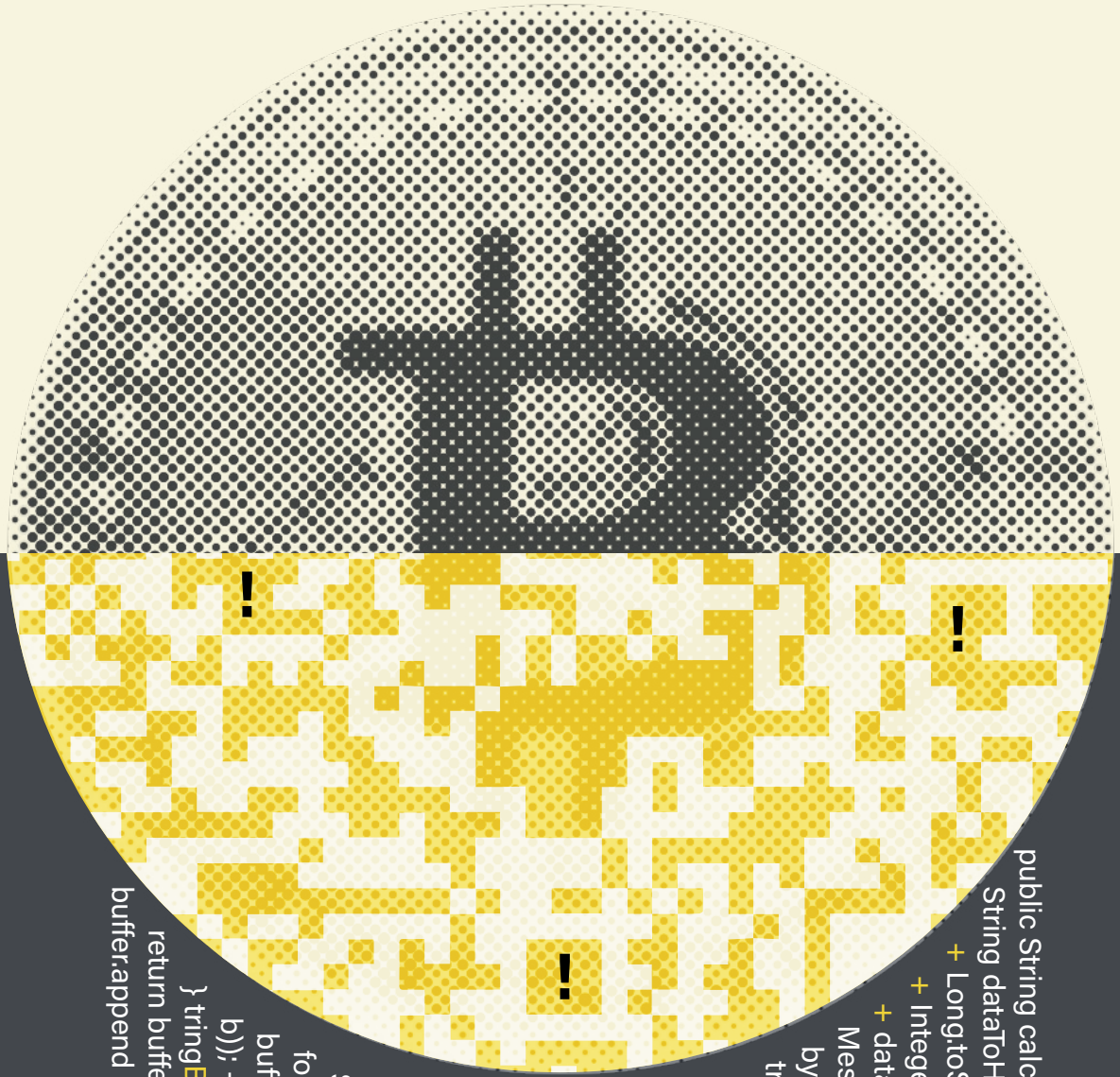
A Guide to Anti-Money Laundering for Crypto Firms

A step-by-step guide to risk mitigation and regulatory compliance best practices



COMPLY ADVANTAGE®

Introduction: Crypto AML Regulations

The AML and regulatory landscape for crypto firms is changing rapidly. This creates both challenges and opportunities for compliance teams.

Regulatory Landscape

Explore the latest regulatory trends and developments in major global crypto hubs, from the United States to the European Union to Australia, China, Singapore and Japan.

Building an AML Program

A step-by-step guide to building an AML program for crypto firms - including a risk assessment, personnel, technology, stakeholder management and expansion into new markets.

Emerging Use Cases & Threats

From DeFi to ransomware, fraud and sanctions evasion, crypto compliance is littered with a host of opportunities - and risks.

Success stories

Meet some of the crypto firms working with ComplyAdvantage to enhance their transaction monitoring, customer screening and ongoing monitoring systems.

Introduction

Welcome to ComplyAdvantage's guide to anti-money laundering (AML) for crypto firms.

The year 2021 was pivotal for cryptocurrencies, non-fungible tokens (NFTs) and other digital assets. Crypto's market cap hit all-time highs in late 2021, and NFTs have attracted attention from retail investors and established investors alike. These trends speak to a broader shift toward DeFi, or decentralized finance, which leverages blockchain technology to execute peer-to-peer transactions. Such transactions bypass the payment and money transfer rails of traditional financial institutions. And this has led to the introduction of a whole new set of financial services and products.

But as cryptocurrencies continue to enter the mainstream in 2022 and beyond, regulators, the media and policymakers are paying more attention to the financial crime risks associated with them. What are those risks, and how can crypto firms work with regulators to manage those? While the regulatory landscape is far from settled, and each jurisdiction will vary in its approach, several trends have started to emerge that will inform a crypto firm's approach to financial crime and compliance.

This guide, which is the product of numerous interviews we conducted with professionals operating in the crypto space, is intended to serve as a practical, hands-on resource. It covers the essentials of building and scaling a crypto AML program and navigating regulatory changes. In addition, it explores some of the emerging use cases — and threats — compliance teams should look out for as they develop and improve their AML/CFT frameworks.

AML/CFT Compliance and Crypto

Cryptocurrencies, NFTs and DeFi have ushered in a wave of innovation, including new asset classes and financial products. Yet these innovations also come with risks, particularly with respect to how criminals can exploit them for their gain. As a result, making sure that crypto firms implement strong anti-money laundering controls has become a top priority for regulators and policymakers.

There is considerable overlap between the AML/CFT compliance considerations fiat-based financial services companies must address and those crypto firms face. A solid risk-based approach is crucial and hinges on conducting a thorough risk assessment — and then revisiting that assessment periodically. Hiring the right personnel and engaging in productive dialogue with regulators is also key when trying to comply with rapidly evolving regulations — especially since these regulations may necessitate changes to a firm's AML/CFT compliance program and its products and services. Many financial crime typologies are also similar: layering, money muling, cybercrime, among others, are universal concerns across the financial industry.

However, there are nuances and areas where those considerations diverge or have a different emphasis. An evolving regulatory landscape may mean incremental changes and tweaks to existing frameworks, or it may involve entirely new crypto-specific regulations. Further, how money laundering typologies and threats manifest themselves can be vastly different within the crypto space. Dusting, off-chain transactions and the use of anonymity-enhanced cryptocurrencies or unhosted wallets add a layer of complexity not found when dealing with strictly fiat-based money flows.

There is also little room for error when addressing these risks. As crypto's profile has risen, so has the scale of potential threats. Leveraging crypto for large-scale sanctions evasion, terrorist financing, cybercrime and layering is becoming increasingly common — a trend regulators are keeping a watchful eye on.

Therefore, the consequences of AML non-compliance for crypto firms are severe. Firms found to have lax oversight may incur hefty fines and face significant reputational damage. Regulators may require an overhaul of AML/CFT processes and, in severe cases, may decide to revoke a firm's license to operate.

As governments globally continue to map out their regulatory frameworks for cryptocurrencies and as financial crime tactics evolve, firms will soon face an inflection point. Understanding where the AML compliance landscape is now — and where it's likely to go in the months ahead — will help firms prepare.

Regulatory Landscape

The regulatory challenges faced by crypto firms are numerous, growing, and different in almost every jurisdiction.

Global

Crypto firms face numerous regulatory challenges. There is currently a flurry of activity in the cryptoasset regulatory space, with the need to regulate these assets made more urgent by the Russian attack in Ukraine and the possibility that crypto could be used to circumvent sanctions. However, the biggest challenge that crypto firms operating across multiple jurisdictions continue to face is the lack of standardized regulation across countries and differing approaches to how to treat cryptoassets.

Governments have adopted divergent approaches to regulating cryptoassets to such an extent that Japan recently called on the Group of 7 (G7) to create a common framework to regulate digital currencies, including cryptoassets. This will include a "need to balance privacy and money-laundering concerns."

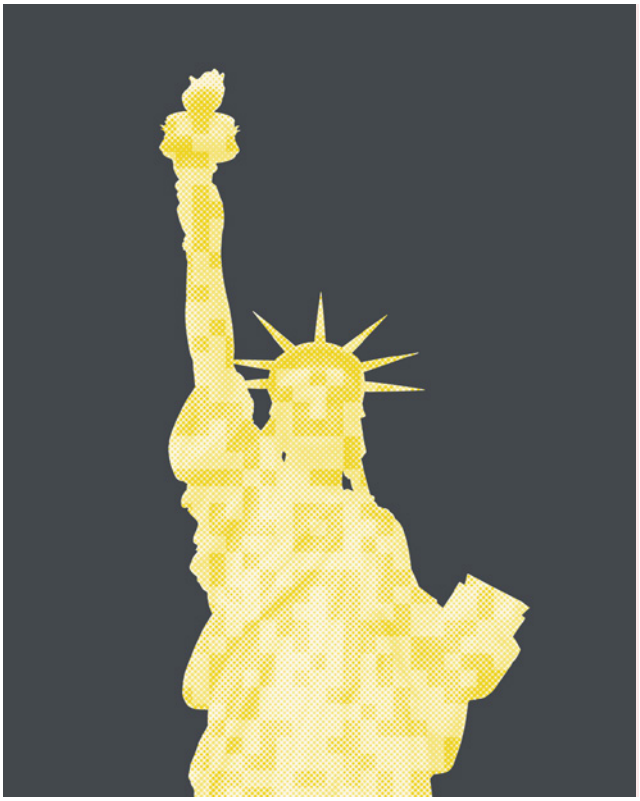
In addition to the lack of standardization of approaches to the crypto industry are the following additional challenges:

- Speed of development of laws and regulations, combined with limited consultation of the industry to understand the practical impact
- Lack of clarity on how the legislation applies to innovations in the crypto space, such as DeFi and NFTs, which could create onerous requirements and stifle innovation
- Bans on mining or cryptoassets, proposals to curb energy use and black swan events, such as the war in Ukraine, could threaten the industry

This section looks at key jurisdictions with fast-moving regulatory developments. Firms must remain abreast of proposed changes to existing laws, new laws, regulatory notices and fines to ensure that they are prepared for the regulatory tsunami that is coming.

United States

Cryptoasset providers are currently treated as issuers of securities, money service businesses (MSBs) offering "convertible virtual currencies" (CVCs) and digital assets with legal tender status (LTDAs), or alternative trading systems (ATS). The Anti-Money Laundering Act 2020 (AMLA) brought



into the scope of the Bank Secrecy Act any providers that deal with virtual assets and digital assets.

This means that firms that process transactions linked to "value that substitutes for currency" must have in place AML/CFT frameworks that comply with the BSA.

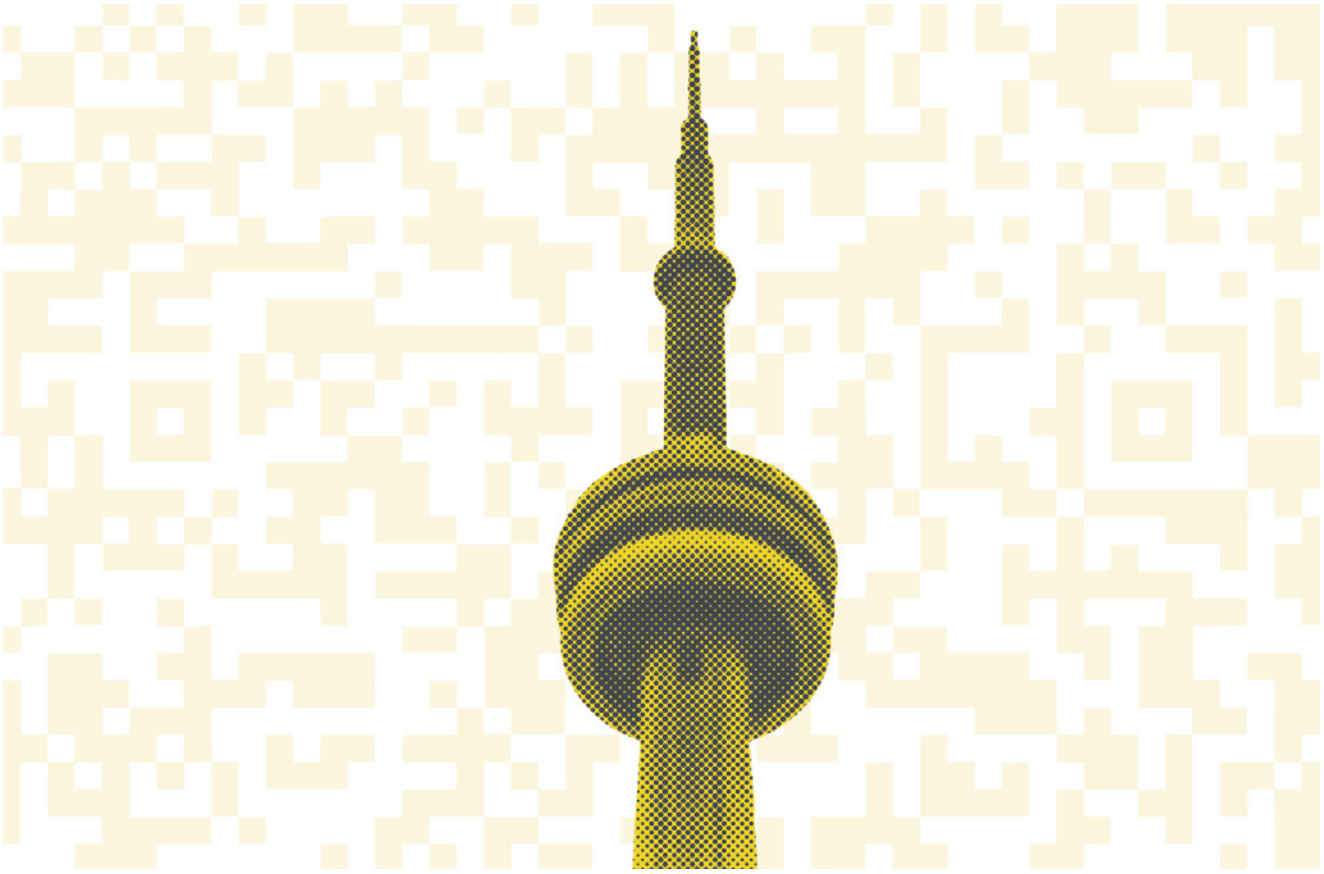
However, crypto regulation in the US is evolving at a fast pace. In early 2021, FinCEN issued a notice of proposed rulemaking detailing reporting and record keeping "requirements for certain transactions involving convertible virtual currency or digital assets" valued at more than $10,000. This includes requirements that apply to both unhosted wallets and wallets that have been hosted in a jurisdiction identified by FinCEN. In early 2022, the SEC proposed changes to how "exchanges" are defined, which could have massive implications for the DeFi space, although there is talk of introducing "safe harbor" provisions as the SEC determines how to continue to treat cryptoassets.

In March 2022, President Biden signed an Executive Order on Ensuring Responsible Development of Digital Assets (EO). The EO sets out a whole-of-government strategy to "support innovation," listing priorities including protecting users, financial stability, national security and mitigating climate change. Among the six priorities is a focus on mitigating illicit finance and national security risks by "by directing an unprecedented focus of coordinated action" across US government agencies and working with "allies and partners to ensure international frameworks, capabilities, and partnerships are aligned and responsive to risks."

Firms also need to also be aware of regulatory expectations around AML/CFT controls that are issued in notices, advisories and fines. For example, in February 2021, OFAC reached a $507,000 settlement with BitPay for processing payments on behalf of merchants that were dealing with digital currency transactions originating in Cuba, North Korea, Iran, Sudan, Syria and Crimea. OFAC found that BitPay should have in place IP geolocation blocking. FinCEN has issued several advisories to address illicit finance risks associated with crypto, ransomware and sanctions.

Canada

In Canada, providers of cryptocurrency offerings (CCOs) fall under requirements for issuers of securities and dealers in virtual currencies must register as MSBs. Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) brought "dealers in virtual currencies" in scope



and applies to both businesses based in and which do not have a place of business in Canada dealing in virtual currencies for their clients in Canada. Measures include carrying out customer due diligence, including "ascertaining the source of funds or of virtual currency in any financial transaction," monitoring transactions, meeting record-keeping requirements and reporting suspicions to FINTRAC, Canada's Financial Intelligence Unit.

Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFRs) sets out additional requirements. These include the need to keep virtual currency transaction records for transactions greater than CAD$10,000, including date of receipt, amount received, name and address of persons involved in the transaction, types and amounts of virtual currencies involved, exchange rates used, identifiers and reference numbers. Canada also introduced travel rule requirements to retain originator and beneficiary information in virtual currency transfers.

The European Union

Cryptoassets are currently regulated for AML/CFT under the 5th Anti-Money Laundering Directive, which brought into scope a requirement for crypto-to-fiat exchanges and custodial wallets to comply with the EU's AML/CFT framework. With regards to licensing, cryptoassets must register with the local regulator as either an MSB, e-money provider or provider of securities. However, many changes are afoot within the European Union in the space of crypto regulation.

The EU introduced a legislative package that sets out new AML/CFT measures tthat will apply to Europe. Specific measures aimed at the crypto industry, or rather, "cryptoasset service providers" (CASPs), are sprinkled across the various pieces of legislation, which also reference the EU's Markets in Crypto Assets Regulation (MiCA). The "new" 6th Money Laundering Directive (6AMLD) covers licensing, regulation and supervision. It highlights that CASPs must be authorized in their home countries and lays out requirements for CASPs operating under the freedom to provide services in the EU. These CASPs, which are not established in, but offer services in, other EU countries, must appoint a contact person in-country and notify the supervisor. Group-wide policies and procedures must be developed to manage cross-border risks. And where an entity operates in multiple countries, the home country has responsibility for enforcing AML/CFT compliance breaches.

The regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing deals with obliged entities in the private sector. The AML/CFT regulations have defined a cryptoasset more broadly as "a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology." It has also expanded the scope to cover additional CASPs that must comply with AML/CFT requirements when the regulation is live to providers of the following services or activities:

- The custody and administration of cryptoassets on behalf of third parties
- The operation of a trading platform for cryptoassets
- The exchange of cryptoassets for fiat currency that is legal tender
- The exchange of cryptoassets for other cryptoassets
- The execution of orders for cryptoassets on behalf of third parties
- Placing of cryptoassets
- The reception and transmission of orders for cryptoassets on behalf of third parties
- Providing advice on cryptoassets

The regulations further prohibit anonymous cryptoasset wallets.

The EU reissued its transfer of funds regulation as the "Regulation on information accompanying transfers of funds and certain crypto-assets" to bring CASPs in scope of payments regulation. The draft regulation has been updated to deal more effectively with the cross-border nature of fund and asset transfers, to ensure traceability of transactions through the payment chain and to more effectively manage AML/CFT risks for holders of cryptoasset and the financial sector. It was updated to incorporate changes introduced by the Financial Action Task Force (FATF) on the travel rule, which requires that certain information accompany wire transfers, and was extended to transfers of cryptoassets. CASPs will be required to identify and hold originator/payer and beneficiary/

payee information and provide this information to law enforcement authorities upon request. One-off transfers that exceed €1,000 must be accompanied with the name of the beneficiary and originator as well as the respective account numbers.

News sources indicate that the EU is considering a shorter implementation period of key legislation to address illicit finance and sanctions risks. MiCA was tabled as a proposal to regulate cryptoassets to address financial stability and consumer protection concerns. However, it has launched debates into energy efficiency with proposals including a ban on proof of work protocols, which would have had wide reaching and severe consequences in the crypto industry had it been approved. Questions remain around what body will regulate which type of cryptoasset, with proposals for the European Securities and Markets Authority expected to supervise stablecoins and the European Banking Authority to maintain oversight of e-money tokens. However, no final decision has been made.

United Kingdom

In the UK, the government has announced that it plans to make the UK a global cryptoasset technology hub. This includes bringing stablecoins in scope of legislation as a "recognized form of payment," developing a "financial market infrastructure sandbox" to support innovation, establishing a cryptoasset engagement group and working to issue a non-fungible token. The UK defines cryptoassets under the Money Laundering Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as cryptoasset exchange providers and custodial wallet providers. As part of its review of economic crime legislation, the government is reviewing cryptoassets. This includes a review of the current definition of cryptoassets in Schedule 9 of the Proceeds of Crime Act to identify if it addresses emerging uses of cryptoassets and non-fungible tokens (NFTs). The legislation will address asset tracing and recovery, legal barriers to adopting new technology, information sharing and gathering, and proliferation financing. The final legislation is also expected to include updates to the AML/CFT provisions regulating cryptocurrencies (including the adoption of the travel rule) and expand the scope of AML/CFT legislation to cover stablecoins. HM Treasury will publish the outcomes in 2022.

The UK's regulator, the FCA has issued Dear CEO letters on managing cryptoasset risks and also recently issued a joint statement from UK financial regulatory authorities on sanctions and the cryptoasset sector setting out legal and regulatory requirements in firms, steps to reduce the risk of sanctions evasion and reporting obligations to the Office of Financial Sanctions Implementation (OFSI) and the UK's Financial Intelligence Unit, the National Crime Agency. With regards to supervision, however, as of April 2022, the UK has only authorized 39 cryptoasset firms. It has indicated that this is largely due to firms not meeting AML/CFT requirements.

Germany

As an EU member state, Germany's cryptoasset regulations will be harmonized when MiCA becomes law, expected later in 2022. Currently, the country's definition of cryptoassets is set out in the German Banking Act (KWG). The KWG was amended in January 2020 as part of Germany's implementation of 5AMLD, defining cryptoassets in broad terms. This includes currency tokens as well as security tokens used for investment purposes. As a result, licenses are required for crypto exchange platforms, and other services related to tokens classified as crypto assets.

When it comes to the prevention and detection of financial crime, the Anti-Money Laundering Act (GwG) is Germany's primary anti-money laundering regulation. Following the changes to Germany's definition of financial services, crypto custody businesses are now subject to the GwG. The GwG defines crypto custody businesses as any firms responsible for the "customer, management and protection of crypto-assets or private cryptographic keys which are used to keep, store or transfer cryptoassets for others." Firms subject to the GwG must meet its requirements across three core pillars: risk management, customer due diligence and suspicious transaction reporting.

France

As with Germany, France's cryptocurrency regulatory frameworks will be shaped by the implementation of MiCA. However, the PACTE Act, introduced in 2019, set out definitions for digital assets. The definitions used are intentionally broad, covering cryptoassets and cryptocurrencies. The PACTE Act also sets out a list of services covered by its terms, including custody of digital assets, the purchase or sales of digital assets against legal currency, the purchase or sale of digital assets against other digital assets, and the operation of a digital assets trading platform.

The storage of digital assets, buying or selling of digital assets in legal tender, the exchanging of digital assets for other digital assets, or operating a digital asset trading platform all require registration from the financial markets authority under L.54-10-2 of the Monetary and Financial Code. From December 2020, the obligation to comply with AML/CFT measures was also extended to all transactions related to crypto-to-crypto exchanges.

As a result, digital asset service providers operating in France should ensure they have an AML/CFT system and internal controls in place. This includes asset freezing, as well as appropriate organizational policies and procedures. These should include:

- Prohibiting the holding of anonymous accounts (KYC obligation from the first euro)
- Criminal liability of managers
- Reporting of transactions to Tracfin (any transaction over 1,000 EUR, and transactions considered to be suspicious)

Cryptoassets are treated as either financial products regulated by the Australian Securities and Investment Commission (ASIC) or as consumer products regulated by the Australian Competition and Consumer Commission (ACCC). Cryptoasset exchanges or cryptoasset secondary service providers (CASSPrs) are registered with AUSTRAC for AML/CFT purposes. The Treasury has recently issued a consultation on CASSPRs licensing and custody requirements, which requests feedback on a proposed licensing regime for CASSPrs, custody obligations to safeguard private keys and the classification of cryptoassets. It calls for views on the current definition and sets out the cryptoassets that are covered by the licensing regime for "entities providing retail consumers with access to cryptoassets which are not financial products" that:

- Operate as brokers, dealers or operate a market for cryptoassets
- Offer custodial services in relation to cryptoassets

It further sets out regulatory expectations for CASSPRs that wish to be licensed as well as steps that can be taken as part of custody obligations to safeguard private keys. The objective is to make the "regulatory framework that is better, safer and more secure."

Singapore

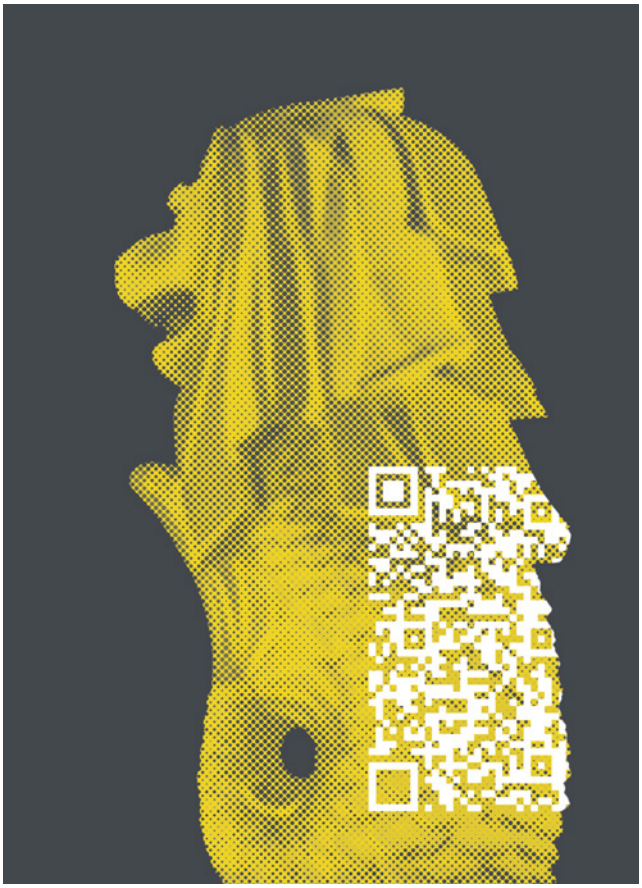
Cryptoassets are regulated in Singapore under the Payment Services Act (PSA) as "digital payment tokens" (DPTs) and cryptoasset providers are regulated as "digital payment token services." They must be authorized by the Monetary Authority of Singapore (MAS). Cryptoassets can also be treated as capital markets products. DPTs are subject to AML/CFT requirements under the MAS Notice PSN02 on the Prevention of Money Laundering and Countering the Financing of Terrorism – Digital Payment Token Service, which includes requirements around risk assessment, CDD, reliance on third parties, correspondent accounts and wire transfers, record-keeping, SARs and internal policies and procedures including audit and training. MAS also published guidelines providing further details on how DPTs should implement Notice PSN02.

Singapore recently passed the Financial Services and Markets Bill 2022 (FSM Bill) to bring into scope of local regulation cryptoasset service providers physically based in Singapore but which only offer services abroad. This was done to mitigate the risk of regulatory arbitrage, align to FATF standards on VASPs and manage Singapore's reputational and AML/CFT risk. These types of businesses "will be regulated as a new class of FIs" subject to licensing and oversight by MAS. The scope of DPT service providers, which previously covered those dealing in DTs and facilitating the exchange of DTs, has also been expanded to cover the following services:

- Inducing or attempting to induce any person to enter into or to offer to enter into any agreement for or with a view to buying or selling any DTs in exchange for any money or any other DTs (whether of the same or a different type)
- Accepting DTs for the purposes of transmitting, or arranging for the transmission of, the DTs
- Safeguarding of a DT or DT instrument, where the service provider has control over the DT or over one or more DTs associated with the DT instrument
- Financial advice relating to the offer or sale of DTs

The FSM Bill also introduced additional licensing requirements, gave MAS the power to carry out regulatory inspections and allowed for coordination between MAS and domestic authorities as well as foreign AML/CFT supervisors. The FSM Bill will also give MAS the ability to issue requirements on technology risk management (TRM), with a maximum penalty set at S$1 million.

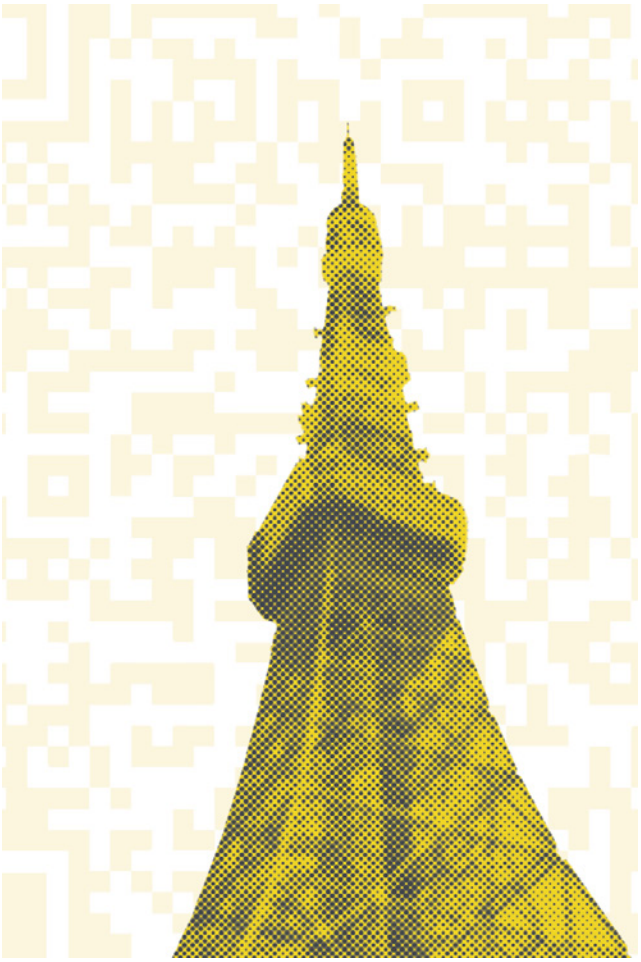
MAS further clarified that it "considers all transactions relating to DT services to carry higher inherent ML/TF risks due to their anonymity and speed." In January 2022, MAS issued Guidelines on Provision of Digital Payment Token Services to the Public [PS-G02], which set out expectations that DPTs should not market or advertise DPT service to the general public in Singapore, indicating that trading DPTs is "highly risky and not suitable for the general public."



China

China has taken numerous steps to crack down on cryptocurrency trading and mining. No cryptocurrencies, except for the country's own digital yuan, are recognized as legal tender, with the People's Bank of China (PBOC) banning cryptocurrency transactions in September 2021. The PBOC has indicated that it has banned cryptocurrencies to tackle financial crime but also to promote economic stability.

Chinese officials set out their position last year indicating that they would "severely crack down on illegal securities activities, and severely punish illegal financial activities." China also took significant action throughout 2021 to crack down on mining, banning miners from carrying out activities. Additional steps that China has taken includes launching a whistleblowing program to allow people to report Bitcoin miners and actively shutting down exchanges. Moreover, while financial and payment companies are forbidden from providing crypto-related services, individuals are not yet banned from holding crypto.



Japan

Japan was one of the first countries to introduce crypto-specific regulations, with different types of tokens subject to different types of regulation. Cryptoassets have their own regulated status in Japan, with cryptocurrencies and value transfer tokens falling under the definition of "crypto assets" in the Payment Services Act. Crypto exchanges are required to be registered as cryptoasset exchange services providers (CAESPs) with the Financial Services Agency (FSA). Security tokens are defined as electronically recorded transferable rights to be indicated on securities (ERTRISs) under the Financial Instruments and Exchange Act (FIEA). Providers of services linked to securities tokens are required to register as Type I Financial Instruments Business Operators (Type I FIBOs).

Stablecoins can be classified as cryptoassets. However, if a stablecoin involves a fiat payment, it can be classified as "kawasetorihik," or a means of payment in fund remittance transactions. Money laundering requirements related to CAESPs are detailed in the Act on Prevention of Transfer of Criminal Proceeds (APTCP). Obligations include: Verifying and recording the identity of customers for certain transactions (exceeding YEN100,000 in value or regular services); recording transactions; reporting STRs to the FSA; and keeping customer information up-to-date.

Recent news reports indicate that Japan is looking to bring crypto exchanges into the scope of its foreign exchange and trade law to manage sanctions risks related to Russia. The FSA had previously shared that it was looking to introduce more stringent requirements in the crypto space, and had set up a dedicated unit and panel of experts to oversee crypto businesses. In March, the FSA requested that crypto firms make their monitoring more robust, identify if recipients of funds are linked to Russian sanctions, and report transactions linked to sanctions.

Tackling the Travel Rule

The travel rule is one of the most notorious crypto compliance challenges. Unfortunately, there is no one-size-fits-all solution — firms need to explore different solutions that have been developed to address it. Firms should ensure that they are able to collect and hold data in a standardized format similar to the data schema developed by the InterVASP Messaging Standards (IVMS-101). For firms that do not have a massive number of clients, they may consider developing a manual work-around, which should include a requirement for those sending transactions to capture both originator and beneficiary data.

However, firms who are strictly focused on implementing the travel rule must ensure that they are following and planning for other regulatory developments. The amount of attention lawmakers and regulators are placing on this industry is astronomical and leading to a deluge of regulatory consultations, new laws, regulation, advisories and licensing requirements for cryptoasset service providers. This means that firms must be able to show that they have comprehensive AML/CFT frameworks that are fit-for-purpose to meet licensing requirements that go beyond the travel rule. While compliance with the travel rule is important, it forms a very small part of the overall AML/CFT program. Documenting AML/CFT policies, procedures and the rationale for bringing in different types of technology and resources is very time-consuming and must cover all aspects of a program, from risk assessment to onboarding, ongoing monitoring (including transactions), SAR/STR filing and record-keeping. Firms must also ensure that they have in place all relevant documentation and personnel in order to comply with general licensing requirements.

Getting ahead of new regulations

With new regulations being announced frequently, firms of all sizes need to devise a strategy for staying ahead of the latest developments. Three key steps to take include:

1. **Horizon scanning:** There is a swathe of regulation that is being introduced in the next year that will impact how the industry innovates and evolves in the next few years. AML/CFT teams should ensure that they are constantly monitoring events and incoming legislation to identify new requirements, threats and risks but also opportunities and plans to tackle these head on. Staying ahead of the curve and making sure that the AML/CFT team has the adequate budgeting approved by senior management to address changes and that the right level of resourcing has been allocated to address regulatory changes is key.

2. **Understand new requirements and impact:** Crypto firms should take the time to fully understand new requirements and the impact on their operations. For some firms, this may mean introducing an entire AML/CFT program into a jurisdiction where they may not previously have been required to have such a thing in place. In other jurisdictions, this may be refining certain aspects of the AML/CFT program or introducing new requirements. It could also mean blocking certain assets, adding a technology layer or developing a strategy to exit a pool of clients who are suddenly deemed to be breaking the law. And lastly, crypto firms may need to comply with regulation that is not crypto-specific, such as sanctions measures, and need to ensure that they have the right controls in place to manage these risks.

3. **Contribute to regulatory consultations:** Crypto firms should try to ensure that they are contributing to legal and regulatory consultations and notices of rulemaking around the globe. This will help show the regulator that they are engaged and understand what is coming. This will also help to ensure that laws and regulations are being developed that do not stifle innovation or lead to the development of laws and regulations that could have a serious negative impact on the industry. This could be done independently or via industry bodies.

Building an AML Program

A step-by-step guide to developing a sustainable AML program for crypto firms, based on interviews with those operating in the sector.

Risk Assessment

Strong money laundering controls begin with a comprehensive risk assessment. As Greg Wlodarczyk, the managing director of virtual assets and new payment methods at FINTRAIL, says, the risk assessment is "a cornerstone for any firm."

While this recommendation isn't unique to crypto firms, it is particularly critical in light of the greater media and political scrutiny faced by crypto firms and the fragmented and rapidly evolving regulatory landscape. And this applies to firms that are currently not under the scope of such regulations, Wlodarczyk continues:

> With regulations changing all the time, you can find yourself a regulated entity overnight.

The risk assessment is an opportunity to identify the AML/CFT risks a crypto firm faces and design a plan that effectively mitigates them. While the overarching considerations are similar to other financial institutions — a firm must assess its risks vis-à-vis the products and services offered, customer base and both the jurisdiction where it operates and where its customers are — there are nuances. These include:

- **Emphasizing proper onboarding processes**
  It is often difficult, if not impossible, to stop transactions on the blockchain once initiated. As result, many firms we spoke with confirmed they found value in introducing greater friction during the initial know your customer (KYC) process for onboarding, including sophisticated identity verification checks.

- **Tracing the flow of money**
  With transaction history recorded via a public ledger, crypto firms have more visibility into the flow of money than traditional banks working with fiat currencies. However, the dilemma becomes: how far back should crypto firms go?

  For example, if a coin (or a fraction of a coin) can be traced back to a sanctioned entity 20 transactions ago, should the current transaction be considered suspicious or illicit? The answer depends on both regulatory expectations and the crypto firm's risk appetite. Proper configuration of transaction monitoring systems and transparency around the approach taken are paramount.

- **Anticipating regulators' expectations**
  Each regulator will have different priorities and levels of knowledge about the crypto space. It is also worth noting that regulators are still learning the use cases for crypto, how it can be used and abused and how it

might fit into wider AML/CFT frameworks. Anticipating a regulator's expectations by examining draft guidance, calls for feedback and other materials can help a firm develop a risk assessment that satisfies compliance obligations.

- **Undertaking a virtual asset risk assessment**
  In some jurisdictions, this type of risk assessment may be mandatory. There may also be specific guidelines to follow and information to document. Irrespective of local requirements, crypto firms should examine the virtual assets they deal with and understand the risks each one poses.

In addition, firms must keep in mind that the risk assessment isn't a one-and-done requirement, but rather should be viewed as a living document. Crypto firms should revisit the risk assessment regularly: at minimum, they should conduct a review annually, but often, even more frequently is better.

Experts we interviewed suggested that a best practice would be to establish specific trigger points that would necessitate a review. Such triggers could include, for example, when considering whether to launch new products or offer a new virtual asset, when expanding into new jurisdictions, when there are changes in regulations or when a new national risk assessment is published. These events may necessitate merely tweaks to existing controls and processes, but they may also require entirely new ones.

It is, therefore, also critical that risk assessments directly connect to a firm's existing AML/CFT controls — that is, how well are existing controls mitigating the specific risks laid out in the risk assessment? Otherwise, it is easy to get lulled into a false sense of security. However, it does no good to set fuzzy matching parameters that result in too many false positives, for instance, or that are not calibrated to flag the right risky customers or transactions.

Typologies

Many of the AML/CFT typologies that crypto firms encounter are the same as those encountered by all financial institutions. Money mules, fraudulent accounts, identity theft and account takeover fraud, among others, are concerns shared across the board. Typologies may also vary in individual markets — some firms told us they will leverage FATF typologies where they're entering new markets and don't have historic customer data to work from. Overall, however, the firms we interviewed highlighted the below as top priorities to address:

- **Layering:** In our interviews, this typology featured prominently as one of the most challenging crypto threats. It can take many forms, such as:
  - Chain-hopping — Involves converting one cryptocurrency into another and moving from one blockchain to another.
  - Mixing or tumbling — Involves the blending of various transactions across several exchanges, making transactions harder to trace back to a specific exchange, account or owner.
  - Cycling — Involves making deposits of fiat currency from one bank, purchasing and selling cryptocurrency, and then depositing the proceeds into a different bank or account.

Multiple rapid trades between different tokens, especially if those trades don't make sense when examining broader market trends, and a pattern of lower-value transactions that are all below reporting thresholds may also indicate layering.

- **Dusting:** This typology involves making a large number of very small transactions with the intention of tainting as many wallets as possible. That activity, in turn, creates a lot of noise within transaction monitoring systems, adding to alert backlogs and increasing the likelihood that firms will switch off or simply overlook illicit transactions. To combat this, firms must have comprehensive customer screening and segmentation processes to determine where best to focus their investigations.
- **Money mules:** Recruiting individuals to move funds, knowingly or unknowingly, as part of a money laundering scheme was singled out as a significant issue. Some firms noted that they've encountered customer profiles — age, gender or jurisdictional characteristics — that they hadn't expected. Although younger individuals have historically been targets for money muling, these firms have, for example, seen more middleaged profiles connected to possible illicit activity.

- **Off-chain or cross-chain transactions:** Often, money laundering occurs via off-chain networks, where KYC and other AML/CFT safeguards are limited or nonexistent and transactions do not get recorded on the public blockchain ledger.

  For example, illicit actors can leverage the Lightning Network, which involves using an overlay network (i.e., a second layer) on top of the blockchain to open a direct channel between two users, enabling faster payments. The users can carry out an unlimited number of bitcoin transactions with each other or with anyone either party is connected with via another direct channel — all "off-chain."

  Tracing those transactions that involve an off-chain payment system or wallet and verifying the accuracy of customer-provided data can be problematic.

- **Laundering of stolen cryptoassets/NFTs:** This includes assets obtained through hacks, scams, compromised websites, bots and wallets, social engineering via Discord or Twitter and fraud. Laundering can occur over multiple transactions or using blenders and mixers. Money launderers may also use peel chains, where stolen funds are slowly "peeled" from the sender's wallet via a long series of small transactions.

- **Payment for goods and services on darknet markets using cryptoassets:** Assets can be transferred through wallets in centralized exchanges to a decentralized wallet, where assets can be exchanged into privacy coins, which subsequently be used to make purchases on the dark web. It is estimated that darknet market funds amounted to $448 million in 2021.

- **Laundering of crypto wallets:** This can occur when the wallet itself is sold for fiat currency, and the cryptoassets and NFTs transfer to the new holder. The new holder can then use the cryptoassets and sell NFTs without being detected, particularly if the wallet operates independent of an exchange or is held by a trust.

Personnel

Crypto firms told us they face additional pressures to appropriately fill key roles given how critical an effective AML/CFT program can be to their survival. While these firms offer potentially exciting growth trajectories, many candidates may also prefer to work in more traditional, regulated financial institutions. High salary expectations can also be a barrier for smaller firms.

Several of the crypto firms we interviewed mentioned their inclination to look to other firms in the sector for talent. After all, there is value in a deep understanding of the crypto space when evaluating the risk landscape and how to best adapt systems and processes to flag suspicious customers and transactions. However, many other firms we interviewed stressed that this may not always be the best approach. The dynamics and intricacies of cryptocurrencies and other virtual assets, while complicated, can be taught.

Instead, those in the crypto space would do well to expand their talent pool and look for candidates with transferable or complementary skills and knowledge. A well-rounded team may include individuals with backgrounds in areas such as:

- **Traditional finance**
  The regulatory landscape is fragmented, with each jurisdiction treating virtual assets differently. Even within the same jurisdiction, regulators may treat each class of virtual assets differently — for instance, a regulator may regard cryptocurrencies as securities and NFTs as intangible capital assets. However, crypto regulations have tended to align with traditional finance regulations, with FATF as well as regional and national regulators defaulting to expanding those guidelines to encompass virtual assets. Therefore, hiring people who understand how to design or work within a traditional AML/CFT compliance program can provide crypto firms with invaluable insight that may help them map those expectations to their own AML/CFT processes.

- **Policy making and regulatory bodies**
  Often crypto firms and regulators find themselves speaking two different languages. Firms that tap into the expertise of those tasked with creating legislation, policies and regulations may find that it gives them a competitive advantage over other crypto firms because

they have, in essence, an in-house translator. Having someone who understands the regulatory environment will help crypto firms anticipate changes in regulations and successfully meet expectations. Mark Aruliah, Senior Policy Advisor at Elliptic, told us that while regulatory engagement and government affairs isn't "a typical AML skillset, this is something crypto firms will have to move into." He highlighted the importance of hiring someone "with standing" in government affairs.

- **Law enforcement**
  Crypto firms often are a nexus point for traditional finance (and fiat currency) and cryptocurrencies. Many have also introduced conventional products, such as credit and debit cards, that blur the line between the two sectors. This can expose the firm to conventional risks and typologies like ATM or credit card fraud in addition to crypto-related challenges. To bridge potential blind spots and knowledge gaps, many firms have opted to hire personnel with law enforcement and investigative backgrounds. These individuals are well-versed in the fraud risks that fiat currencies pose and can use their experience to anticipate how criminals might abuse crypto products.

General Considerations and Best Practices

Among the experts we interviewed, the most frequently cited must-have skill set for a compliance officer was relationship-building. Given the increasing interest in cryptocurrencies and other virtual assets from consumers and criminals alike, it's clear that the scrutiny of crypto firms will only grow. Managing regulatory affairs and building relationships with regulators will therefore be a significant part of the compliance function of any crypto firm. Hiring individuals with relevant knowledge and experience involves understanding what regulators expect of them and, crucially, how to present that information and make a good impression.

In addition, some experts had a word of warning to share. Many firms in the crypto space consider themselves tech companies first and financial services companies second. That isn't surprising: cryptocurrencies and virtual assets exist because of advances in digital technology, and those who gravitate to this sector share a love for technology. But from a company culture standpoint, this means firms dedicated to offering digital asset products share a few key characteristics with other tech-focused start-ups: a heavy reliance on automation and small teams.

However, that can come at a cost: one of the challenges faced by smaller teams is that when individuals wear many different hats, conflicts of interest and contradictions can arise. There is, for instance, inherent friction between employees tasked with onboarding new customers, where speed and a seamless experience are valued, and those performing the necessary customer due diligence, who may need additional time or documentation to verify a customer's identity.

Other areas of overlap with AML/CFT compliance that may be problematic include data protection obligations and internal auditing processes or hitting revenue targets and other business growth metrics. Compliance officers should be able to remain impartial, and firms should make sure they are implementing appropriate safeguards to foster the objective treatment of AML/CFT compliance issues.

Finally, compliance is complex and often intentionally siloed from the rest of the company, partly due to the need to avoid those conflicts of interest. However, crypto firms need to encourage a culture of prioritizing compliance education. Other departments should be aware of AML/CFT compliance obligations and how they impact their day-to-day responsibilities. And within the compliance department, investing time and resources to document processes, upskill employees and build the team's in-house knowledge will be key. Ongoing training is crucial, particularly given how quickly the compliance landscape evolves. Further, there should be no compliance gaps resulting from anyone deciding to move on from their role and the company

> While regulatory engagement and government affairs isn't "a typical AML skillset, this is something crypto firms will have to move into.
>
> Mark Aruliah, Senior Policy Advisor, Elliptic

Technology

Much of the excitement around virtual assets and blockchain technology more generally stems from the potential to build on these assets to create new products and experiences. It's only natural that companies that focus on virtual assets attract employees interested in developing new solutions — not merely accepting or adapting existing ones. That can lead to a tendency to want to build everything in-house, including AML/CFT compliance solutions. In the build vs. buy debate, crypto firms often land solidly on the build side of the argument.

But for most firms, the time, energy and resources spent building AML/CFT compliance solutions would have been better spent elsewhere. After some trial and error, many firms choose to look externally for compliance tools, concluding that there are existing solutions that serve their needs or that can do so with a bit of tweaking.

Instead of trying to reinvent the wheel, crypto firms should look for solutions that help automate these compliance processes, including:

- **Onboarding and identity verification:** Like other regulated entities in the financial space, crypto firms must perform identity verification checks and KYC measures to establish and verify the identity of their customers. Given that once initiated, crypto transactions can take mere seconds to complete, there is increased pressure to get the on-boarding piece right.

  To mitigate risks, crypto firms would do well to consider using a layered approach to identity verification. For example, firms may choose to conduct an examination of identity documents in addition to a video or photo KYC check as a matter of course. It may also be worth considering slowing down the onboarding process by instituting a mandatory 24-hour wait between onboarding and completing transactions. High-risk customers may prompt the firm to undertake other, more involved due diligence measures.

- **Screening and monitoring:** Even after onboarding a customer, crypto firms must be able to accurately and efficiently monitor their customers for changes. If they have been added to sanctions or watch lists, if there are changes in their politically exposed person (PEP) status, or if the status of any relatives and close associates (RCAs) notably changes, this may necessitate swift action. Additionally, crypto firms would do well to ensure they have the tools needed to detect whether their customers have been involved in adverse media stories, as that might trigger a higher level of scrutiny and monitoring.

- **Transaction monitoring:** This area of compliance is arguably where crypto firms and traditional banking diverge the most. Brandi Reynolds, Managing Director at Bates Group, a consultancy, and outsourced CCO for eToro USA and Voyager Digital NY, says:

> "Firms often do not recognize the importance of transaction monitoring, often over relying on KYC at the expense of other controls.

Firms should remember that "transaction monitoring is critical to an effective AML program," Reynolds told us.

Like banks, crypto firms are expected to monitor and understand the transactional behavior of their customers and scan for suspicious activity. However, the speed with which transactions occur and the variety and volume of data transmitted with each transaction, especially when one cryptocurrency is converted into another, can make it challenging to keep pace. In addition, firms must ensure their transaction monitoring tools are tailored and calibrated to ensure proper scrutiny of transactions where cryptocurrencies are cashed out and converted to fiat currency — something traditional banks don't typically need to prioritize.

It is here where proper segmentation of customers is crucial. Crypto firms should thoroughly examine any personally identifiable information (PII) and leverage behavioral analytics to help profile customers and set rules according to expected behaviors. The more comprehensive a firm's segmentation, the better able that firm will be to assess the level of risk a transaction poses, whether that risk is due to the customer, the counterparty or the jurisdictions involved.

Managing Internal and External Stakeholders

The Executive Team and Board

AML/CFT compliance is often viewed by many in the company as a necessary component of the business but not one that moves the needle from a growth perspective. Given its complexity, the compliance landscape is also not well understood by individuals outside the department. It can, therefore, be challenging to get buy-in for compliance initiatives from the leadership team or to ensure compliance is top of mind when making business decisions.

It may be tempting to lean into the argument that not taking action on compliance will lead to negative consequences, including reputational damage and revocation of licenses. But that line of reasoning will only take compliance officers so far — and won't enable productive conversations or foster a culture of compliance, which is the end goal. Instead, education is crucial. The board and the executive team should come away from conversations about compliance with an understanding of not just what the regulations are but how working within them can benefit the company's bottom line. In one instance, a crypto firm engaged a law firm to support internal conversations around licensing, coaching the firm's founders on what the dialogue with regulators would look like and the kinds of information they would be looking for.

In essence, the compliance team must demonstrate that it is working with the rest of the business to achieve common goals. It is ultimately the compliance officer's responsibility to make it clear to the leadership team — and the company as a whole — how the right AML/CFT strategies can be a competitive advantage.

Regulators

A firm's first contact with a regulator is typically regarding licensing requirements, and that can set the tone for the firm's relationship with the regulator moving forward. To ensure the firm understands expectations around licensing and its compliance obligations, it should review consultations and guidance by local regulators and lawmakers.

For example, the Australian Treasury recently issued a consultation paper detailing licensing and custody requirements, which includes ensuring that "the services covered by the license are provided efficiently, honestly and fairly" and that the market operates in a "fair, transparent and orderly manner." Such guidance is not atypical and underscores that regulators place a high value on transparency — a requirement that doesn't disappear once the license is granted.

Consistent, constructive communication with regulators is vital and mutually beneficial. A crypto firm that builds a good working relationship with regulators is well-positioned to navigate the legal and regulatory landscape. At the same time, the regulator can leverage the crypto firm's on-the-ground experience to enhance its understanding of the industry and create regulations that reflect how crypto is being used in its jurisdiction.

Knowing how to speak to regulators is an important first step to building that relationship, particularly since regulators expect to meet directly with the compliance team. It may be helpful to examine recent policy statements and the regulators' objectives and then consider how a firm's current AML/CFT processes support those objectives. Some firms, for example, have made inroads by appealing to the goal of investor or customer protection since that is a stated priority of many regulators. They have made that the heart of their business and have committed to showing how they safeguard their customers through their AML/CFT program and other processes.

Still, there is no need to over-complicate matters. Many experts we interviewed stressed that it is not always about what is said but how it is said. Therefore, compliance officers must be mindful of what they are being asked. Answer questions concisely, consistently and using language free of internal or crypto-specific jargon. And if there is a breach or compliance gap, reporting it is the bare minimum: what is more important is how the firm will address the issues and within what time frame. Ultimately, regulators want to be

confident that the firm has thoughtfully considered its AML/CFT compliance risks and can mitigate them. The more firms can clearly demonstrate their capabilities in this area, the better off they will be.

It is also worth noting that cryptocurrencies and virtual assets are a new asset class — and few people outside of the industry have a strong or complete grasp of the underlying technology and potential use cases. Crypto firms have an opportunity to engage not just local regulators but the legislative branches of government and the media to educate and drive the narrative around virtual assets. They should take the time and effort to explain key industry terms, their business model and how the technology works. That may, in turn, lead to a constructive regulatory environment that combats illicit crime without stifling innovation within this nascent industry.

Expanding Into New Markets

As more people learn about digital assets and the "wild frontier" of crypto continues to blend with the traditional financial industry, many firms are exploring how best to tap into the new opportunities this presents. But while it is an exciting time to be in the crypto space, it still poses quite a few regulatory challenges — not least of which is that the regulations governing virtual assets are in a state of flux. They also may not immediately cover many of the gray areas that have emerged and will continue to emerge as the sector evolves. Expanding to new markets, products and services requires crypto firms to adapt to a fragmented and rapidly developing regulatory landscape.

It is vital to take an agile approach and adapt quickly to changes, which is much easier if a compliance mindset exists from day one. Experts we interviewed highlighted four areas where firms can put that guidance into practice when considering how to grow their businesses.

1. **Incorporate compliance considerations into the design or research stage**
   When evaluating whether to launch new coins or new products related to virtual assets, it is critical to consider the impact such an action may have on compliance obligations — which will likely differ from jurisdiction to jurisdiction. Crypto firms would do well to adapt their product designs and plans to fit the regulatory landscape instead of trying to retrofit their products to comply with regulations later on. To that end, firms may find it beneficial to take a proactive approach and engage with regulators when developing new products or when trying to understand how a requirement may apply.

   Along similar lines, firms should look ahead to anticipate what kinds of regulatory action may be taken in a firm's current jurisdictions and in jurisdictions to which the firm may want to expand. Regulators often telegraph their actions well in advance with draft legislation and calls for feedback. Even if events don't come to pass as envisioned, conducting this exercise at the planning stages can help firms design products and services that can more easily adjust to regulatory changes.

2. **Establish a presence in the market**
   It is important to be deliberate about expansion plans. Many of the experts we interviewed stressed the importance of establishing a physical presence in jurisdictions of interest and building relationships with local regulators. Seek out local regulatory bodies and lean on the expertise of consultants in the area. Only through considered exploration of the compliance landscape can crypto firms make an educated decision about if it is in the firm's best interest to expand into that market.

3. **Understand how sanctions compliance obligations may change**
   Governments can be very quick to make changes to their sanctions lists, imposing and lifting measures frequently to respond to a number of sometimes conflicting geopolitical pressures. Even when two governments are generally aligned, it is common to see differences in the specific individuals and entities sanctioned, and in the precise scope of those sanctions.

Given recent reports as to how cryptocurrencies can be used to evade sanctions, sanctions compliance will likely be a top priority for regulators when evaluating overall AML/CFT compliance. Crypto firms looking to expand to new markets would do well to pay careful attention to how different approaches to sanctions may impact their operations.

4. **Take steps to reduce "brain drain"**
   While improving employee retention is always beneficial, it can be even more valuable for firms looking to expand into new markets. Launching a new product or service or venturing into new jurisdictions requires immense effort and a steady hand. In addition, maintaining a consistent point of contact with local regulators, someone with which regulators can build a solid relationship, is crucial in these early stages of expansion. Firms that take steps to retain their talent for as long as possible are in the best position to grow the business successfully.

Emerging Use Cases and Threats

Crypto compliance professionals need to be aware of the latest potential risks to their firms.

Non-Fungible Tokens (NFTs)

From artwork to music, collectibles and real estate, the number of use cases for NFTs is growing. Identity management through NFTs, where a person's identity is represented digitally with an NFT, may improve the ability to perform IDV checks. And smart contracts enforced through NFTs may foster more transparent and secure deal-making. But these use cases also pose serious risks. Just as the buying and selling of traditional art, collectibles and real estate have become a haven for money laundering, so can NFTs. In March 2021, a hacker duped a collector in the United Kingdom into buying a fake limited edition Banksy NFT. While the money was returned, the warning is no less relevant. As real estate NFTs gain traction, for instance, it's not too far of a leap to envision a scenario where an NFT version of the Vancouver model becomes a significant threat.

So far, regulators have focused more on cryptocurrencies than NFTs. But as the use cases multiply, there will be increased scrutiny and regulation. Further, regulators will likely diverge on how they define and classify an NFT: in some jurisdictions, NFTs may be viewed as securities or derivatives, while in others, it could depend on what the NFT represents in the physical world. Crypto firms involved with NFTs will want to keep a careful eye out for regulatory developments in this area.

Decentralized Finance (DeFi)

Decentralized finance is the umbrella term for financial transactions that use blockchain technology and smart contracts to facilitate direct, peer-to-peer transactions. These transactions don't rely on traditional intermediaries (i.e., financial institutions) and are often faster, less expensive and can easily traverse national borders.

From DeFi, a new set of financial products and services have emerged. Crypto savings accounts allow users to earn interest at higher rates than they typically receive with fiat currency at a traditional bank. People can obtain a loan within minutes — no paperwork or waiting for approval required — or can act as a lender to their peers. A group of individuals can decide to pool resources to protect against risk independently of an insurance company, which offers an alternative to purchasing insurance through traditional insurance companies.

Yet as the applications for DeFi grow, so too do the risks. Direct peer-to-peer transactions that occur within seconds leave little room for safeguards against abuse. Further, just as in traditional finance, cross-border transactions may also carry higher risk, notably in jurisdictions with high corruption, lax money-laundering controls or where terrorist organizations have a prominent presence.

As DeFi evolves, DeFi platforms and other virtual asset service providers (VASPs) will need to pay particular attention to their counterparty risks and the risks posed by their customers. Transactions involving unlicensed or unregistered VASPs and unhosted wallets are considered highly risky given the challenges around verifying who is conducting those transactions. In addition, these firms should ensure they have implemented robust customer due diligence measures to weed out bad actors before transactions occur.

Emerging Threats

Ransomware

Widespread digital adoption has led to a significant uptick in cybercrime risks, particularly ransomware attacks. These attacks target individuals or businesses, blocking access to critical data on their computer systems until they pay a ransom, often in cryptocurrency.

Worldwide, ransomware attacks increased by 105% in 2021 compared to 2020, and regulators from the US, Asia Pacific and elsewhere have been exploring how to tighten controls and address this threat. It's worth noting that while some targets have been high-profile, such as the San Francisco 49ers and Nvidia Corporation in February 2022 and Samsung, Microsoft, Bridgestone and Toyota in March 2022, cyberattackers are hitting smaller targets as well. School districts, hospitals and health care companies, financial institutions and other entities involved in critical infrastructure projects are among those most at risk of coming under attack.

If the victim complies with the ransom request, firms may notice, for example, a large transaction directed to a sanctioned wallet. However, payments made due to ransomware attacks are not always straightforward. They may involve sending money to different wallet addresses and using mixers and other layering strategies to make it harder to identify and trace the transactions.

Sanctions Evasion

Russia's war in Ukraine and the harsh sanctions issued by many Western countries in response has intensified discussions as to how nations and bad actors can exploit crypto to evade sanctions. While officials say there is currently no evidence that designated Russian individuals or entities have used crypto to dodge sanctions in any material way, it is apparent that regulators are taking this possibility seriously. As a result, crypto firms must ensure they take steps to detect and prevent this activity — or potentially be held liable for potential sanctions violations.

Firms should thoroughly screen new customers against sanctions lists as part of their customer onboarding due diligence and regularly re-screen existing customers. Further, the compliance team should ensure transaction monitoring protocols are calibrated appropriately according to the firm's risk-based approach. Monitoring IP addresses to identify transactions involving high-risk jurisdictions can help detect sanctions evasion activity. Other red flags include making rapid transactions involving multiple wallet addresses and using anonymity-enhanced cryptocurrencies, such as monero, DASH or ZCash, or a cryptocurrency mixing service.

Darknet Markets

These global online marketplaces enable buyers and sellers of illicit drugs, identity information and other illegal goods and services to communicate and transact. The threat that bad actors will exploit crypto firms to facilitate trade in these marketplaces is particularly acute since participants often use virtual currencies as their preferred method of payment. Bitcoin is currently the most preferred cryptocurrency across the different darknet markets. However, monero has grown in popularity recently, and some signs indicate it may overtake bitcoin in the coming years.

As the threat has evolved, governments and law enforcement agencies worldwide have stepped up efforts to disrupt and take down these darknet markets. In April 2022, the United States announced sanctions against Hydra Market, the largest darknet market in the world — this coincided with decisive action by German law enforcement to shut down Hydra servers in the country and seize $25 million in bitcoin.

Fraud

As cryptocurrencies become more widely used, cryptocurrency fraud will increase. Already fraud has proven to be a serious and growing threat: according to a recent report by Chainalysis, $14 billion flowed to addresses linked to criminals in 2021 — nearly double the amount directed to illicit addresses in 2020 ($7.8 billion). Notably, crimes involving scams and stolen funds experienced the most growth.

The Chainalysis report also identified an emerging type of scam called a rug pull. Developers establish themselves as working on seemingly legitimate crypto projects, selling tokens as a way to raise capital, only to abruptly disappear with their investors' money. Given the current lack of investor protections in place for cryptocurrencies, investors are often left holding the bag and can only watch as the token's value falls, further compounding their losses.

Stolen funds also accounted for a significant number of fraud cases in 2021, with scammers stealing approximately $3.2 billion in crypto, primarily from DeFi protocols. This amount is only expected to increase as DeFi projects and use cases multiply.

More generally, the continued development of the crypto sector will inevitably invite more fraud. Scams that are not unique to crypto — including phishing, romance scams, account takeover fraud, invoice redirection and push payment fraud — will find new applications and revenue sources in the crypto space.

Terrorist Financing

Cryptocurrency assets and DeFi feature prominently in terrorist financing efforts. These currencies and technologies enable cross-border transactions with relative anonymity that don't involve an intermediary, settle in minutes and are often very difficult to stop or reverse once initiated. The fragmented regulatory landscape also increases the likelihood suspicious transactions will go undetected, particularly in pockets of the world with lax AML/CFT oversight.

Where cryptocurrencies are used by terrorists and violent extremists, bitcoin often features; however, monero and other privacy-enhanced coins have increasingly been looked at as more desirable alternatives. In the summer of 2020, a large pro-ISIS news website announced it would not take donations in bitcoin anymore, preferring monero instead. Then, in April 2021, a pro-ISIS cybersecurity group, the Electronic Horizons Foundation, issued a warning that transactions made with bitcoin could more easily be tracked.

The use of privacy coins isn't in and of itself a solid indicator of illicit activity. But crypto firms should look at those transactions with a higher degree of scrutiny — especially if the portfolio of one or both of the users involved consists primarily of anonymity-enhanced cryptocurrencies.

Geopolitical Unrest

Geopolitical tensions and domestic unrest can roil the operations of any firm, but this is especially true of crypto. In June 2021, when China banned cryptocurrency mining, operations shifted to other countries. The US became a primary hub, with Kazakhstan coming in second. However, high fuel prices and power shortages, exacerbated by the enormous power consumption required to mine bitcoin, have led to domestic unrest. In response to violent riots and civil unrest, Kazakhstan's government brought in military reinforcements from Russia and cut the internet, causing an immediate shutdown of its bitcoin mining operations.

The internet was restored, and operations have resumed. However, such situations underscore how vulnerable crypto firms are — even in countries considered to be relatively stable — during periods of turmoil. With the world experiencing an uptick in civil unrest and political instability, crypto firms must be ready to react if a situation becomes untenable. Whether its operations are threatened, directly or indirectly via partner companies, or whether the unrest has regulatory consequences, a firm's risk-based approach must account for and mitigate these possible threats to the business.

Conclusion

Compliance professionals will most likely look back on 2022 as a defining year for crypto. If current trends continue, it is set to mark the point at which adoption of cryptocurrencies and regulatory reforms collide, leading to a sector that is more regulated, and increasingly mainstream. Regulatory arbitrage will, however, remain one of the biggest challenges crypto firms must grapple with.

Staying ahead of the regulatory curve, alongside smart investments in AML technologies and a diverse compliance staff, will set crypto firms up for success. Not only will they have better relationships with regulators and policymakers, but productivity will increase, and customers will trust the products and services they offer more.

Paxos

By implementing automated workflows, bitcoin giant Paxos increased the efficiency of its AML screening by 80%. ComplyAdvantage's search algorithms and dynamic AML risk database facilitated this improvement, allowing Paxos' compliance team to focus on whether the customers flagged by the screening solution fit within their risk appetite.

Read about the scalable compliance solution chosen by Paxos here.

Ziglu

ComplyAdvantage's solution for crypto company Ziglu reduced its predicted onboarding time by over 50%. After implementing the ComplyAdvantage RESTful API, checks were completed in seconds, which allowed for both a seamless experience for Ziglu's customers and a reduction in manual back-end compliance checks.

Read about why Ziglu chose ComplyAdvantage as their AML provider here.

UKDE

By introducing an AML screening and ongoing monitoring system, global financial service provider UKDE reduced time spent on remediating alerts by 40%. With a large Chinese client base, UKDE needed a powerful compliance solution that could accommodate non-Latin characters. With its refined AML program in place, UKDE experienced fewer false-positives and incorrect hits.

Read about why UKDE switched to ComplyAdvantage here.

About ComplyAdvantage

ComplyAdvantage is the financial industry's leading source of AI-driven financial crime risk data and detection technology. ComplyAdvantage's mission is to neutralize the risk of money laundering, terrorist financing, corruption, and other financial crime. More than 800 enterprises in 69 countries rely on ComplyAdvantage to understand the risk of who they're doing business with through the world's only global, real-time database of people and companies. The company actively identifies tens of thousands of risk events from millions of structured and unstructured data points every single day.

ComplyAdvantage has four global hubs located in New York, London, Singapore and Cluj-Napoca and is backed by Goldman Sachs Growth Equity Fund, Ontario Teachers', Index Ventures and Balderton Capital. Learn more at:

ComplyAdvantage.com

Our Customers

Santander · GEMINI · OakNorth Bank · CURVE · raisin. · Munich RE · Lydia · OANDA

Get in Touch

AMER

New York

220 5th Avenue,
9th floor
New York
NY 10001

P +1 (646) 844 0841
contact.usa@complyadvantage.com

EMEA

London

165 Fleet Street
London EC4A 2AE
United Kingdom

P +44 20 7834 0252
contact.uk@complyadvantage.com

APAC

Singapore

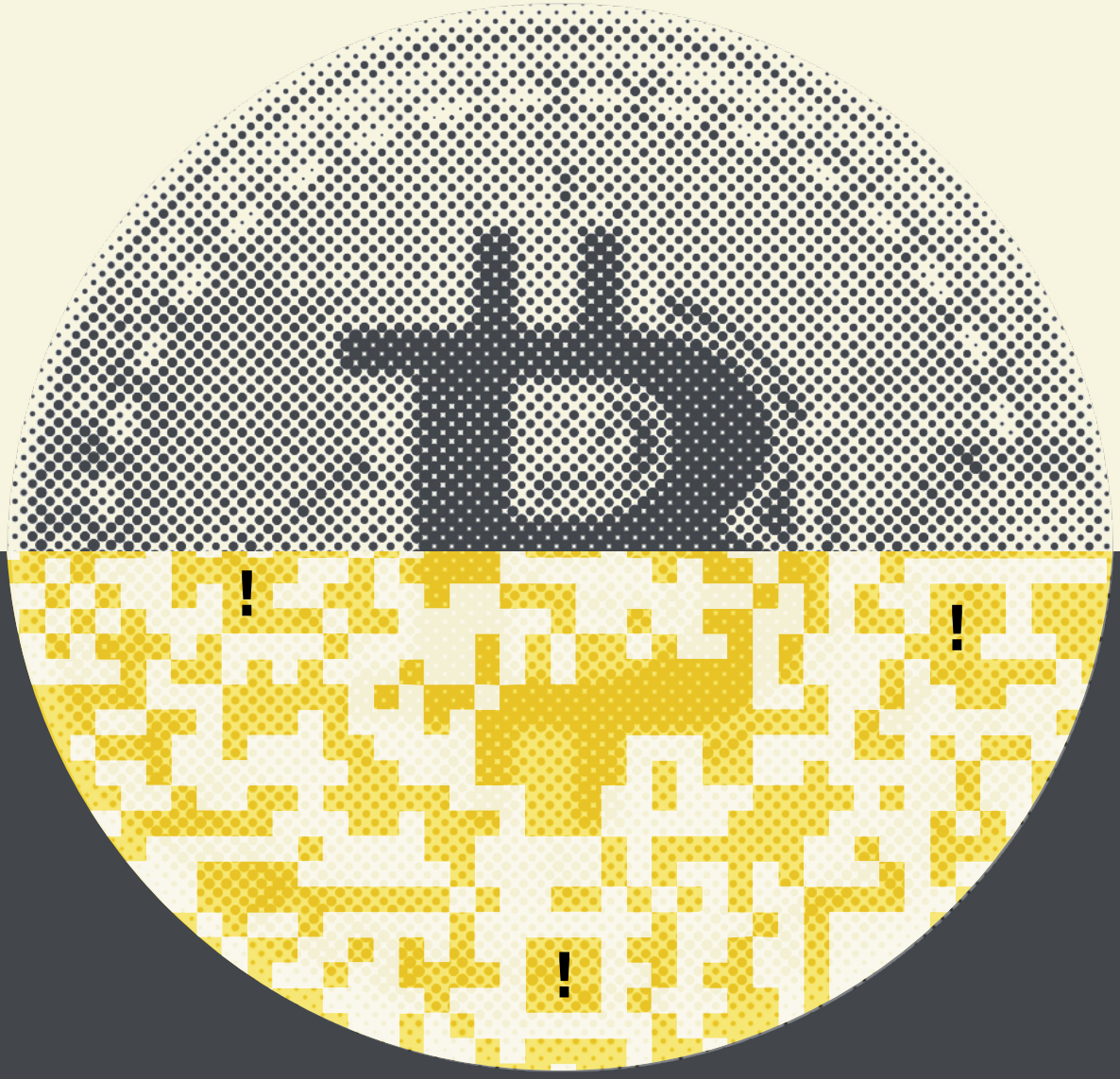
26 China Street
#02-01 Far East Square West Plaza
Singapore
049568

P +65 6304 3069
contact.sg@complyadvantage.com

EMEA

Romania

34-36 Somesului street
Cluj-Napoca
Romania
400145
P +40 752 647 872



For details on the source materials used in this guide, please visit complyadvantage.com/insights