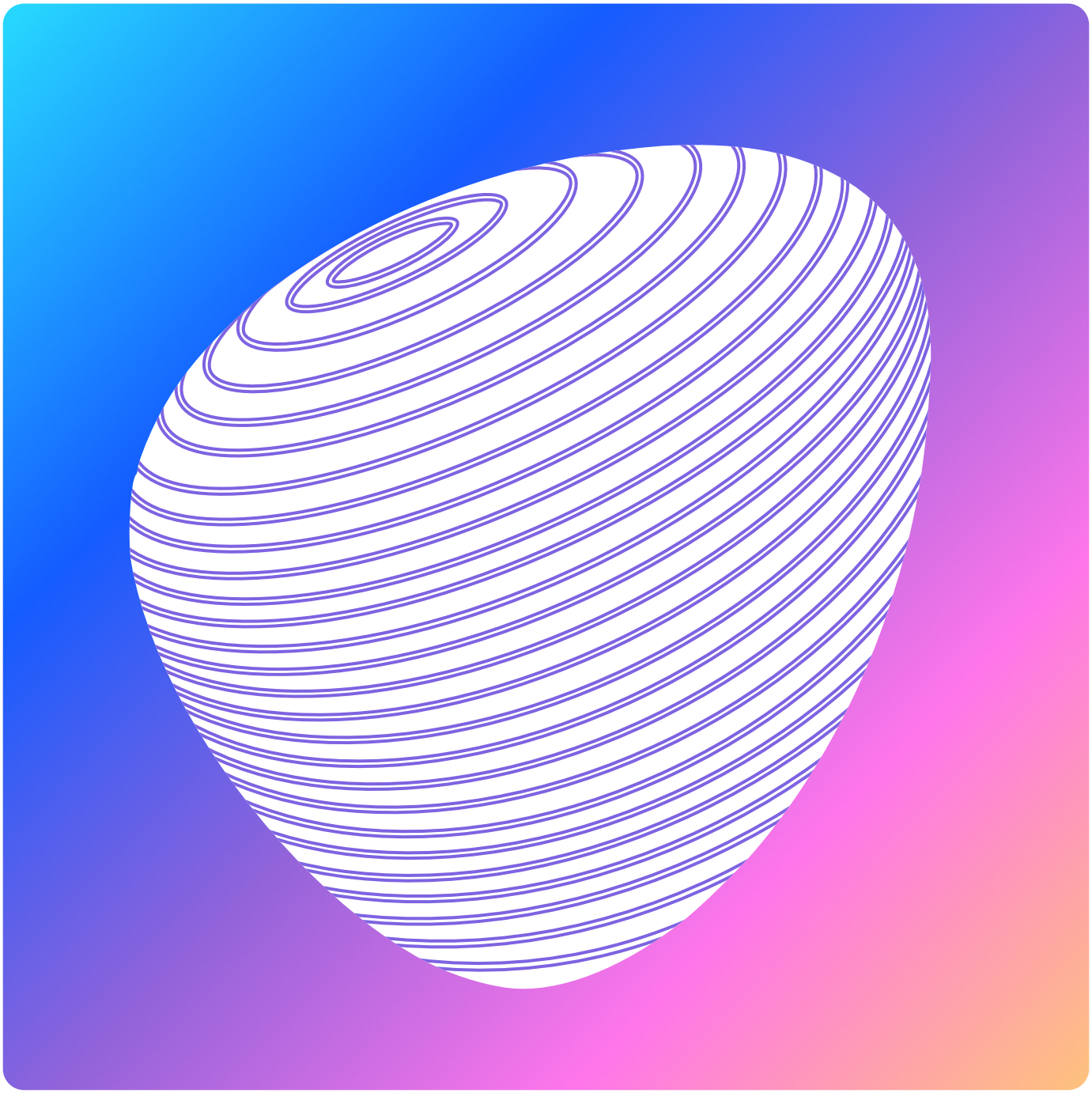
Pebble

The Tacen Beginner's Guide to Crypto Compliance



TACEN.COM — BOOK SERIES

Table of Contents

Pebble

The Tacen Beginner's Guide to Crypto Compliance

Legal Disclaimer

The information provided in this guide does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in this guide are for general informational purposes only. Information in this guide may not be the most up-to-date legal or other information. This guide contains links to other third-party websites. Such links are only for the convenience of the reader, user, or browser; Tacen Inc. does not recommend or endorse the contents of the third-party sites.

Readers of this guide should contact their attorney to obtain advice with respect to any particular legal matter. No reader, user, or browser of this guide should act or refrain from acting on the basis of information on this guide without first seeking legal advice from counsel in the relevant jurisdiction. Only your individual attorney can provide assurances that the information contained herein–and your interpretation of it–is applicable or appropriate to your particular situation. Use of, and access to, this guide or any of the links or resources contained within the guide does not create an attorney-client relationship between the reader, user, or browser and Tacen Inc., or the guide authors, contributors, and their respective employers.

All liability with respect to actions taken or not taken based on the contents of this guide are hereby expressly disclaimed. The content in this guide is provided "as is" and no representations are made that the content is error-free.

Introduction

The digital asset industry started with the introduction of Bitcoin back in 2009. Since that time, the global crypto market cap has reached $2.05 trillion[1] with billions of transactions each year. Unfortunately, with the explosive growth also came abuses, primarily in the form of hackers, money laundering, sanctions evasion, and illicit financing.

To combat these abuses, regulators have imposed traditional financial industry compliance frameworks to the crypto industry and those frameworks have been introduced and steadily developing within the crypto industry.

What is Crypto Compliance?

In its most basic form, Crypto Compliance is defined as:

Following applicable laws and regulations, such as the Bank Secrecy Act (BSA) and its related anti-money-laundering (AML) provisions, to help prevent financials crimes, such as fraud, money laundering, and terrorist financing, by implementing Know Your Customer (KYC) standards, establishing internal systems and controls, conducting independent audits, training employees, and meeting reporting and filing obligations.

1. CoinMarketCap, https://coinmarketcap.com/ (last accessed August 30, 2021).

Why this guide?

This beginners guide will walk you through some of the necessary steps to help you toward crypto compliance. The guide also explains some of the nuances involved in the process, common pitfalls, and penalties for non-compliance.

What can you expect?

This beginners guide will walk you through some of the necessary steps to help you toward crypto compliance. The guide also explains some of the nuances involved in the process, common pitfalls, and penalties for non-compliance.

Who is this guide for?

This guide is for you if you are:

- ✓ New to crypto and want to learn more about crypto compliance;
- ✓ A crypto startup establishing compliance operations; or
- ✓ An established crypto business implementing new compliance operations.

Chapter 1: Past, Present, and Future of Crypto Compliance

Even though the first cryptocurrency was launched back in 2009, little to no regulatory guidance existed in the crypto space until 2013 when the Financial Crimes Enforcement Network (FinCEN) issued its guidance on the application of the BSA to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies[2]. And it wasn't until 2015 that FinCEN U.S. regulatory agency brought a formal enforcement action in the crypto space[3]. Then, following the rise of initial coin offerings (ICOs) in 2017 and a significant increase in the price of bitcoin, governments, agencies, and financial institutions began to take action. This legitimized crypto and led to the need for the development of crypto compliance.

The History of Crypto Compliance

As crypto began to take off, so did enforcement of the BSA by regulators, specifically its AML compliance and KYC standards. While some countries began to impose their pre-existing regulatory frameworks, others started drafting new laws and regulations to govern the crypto industry, and some decided to ban crypto altogether. In response, the exchanges operating at that time began moving to jurisdictions with laws and regulations that were favorable to

2. See U.S. Dep't of the Treasury, Fin. Crimes Enf't Network, FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013) (hereinafter, "FinCEN 2013 Guidance").
3. See In the Matter of BFXNA Inc. d/b/a Bitfinex, CFTC Docket No. 16 - 19, https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual (June 2, 2016).

the crypto industry, and new exchanges became more selective when choosing where to locate their businesses.

Crypto Compliance Today

The number of countries recently adopting crypto compliance frameworks has been accelerating, with the primary focus being AML compliance. As a result, crypto exchanges in some countries have had to comply with AML requirements or face significant fines and even criminal liability.

However, the significant cost of crypto compliance continues to push crypto exchanges to move their operations to countries where regulatory and compliance requirements are lax or non-existent.

The Future of Crypto Compliance

The future of crypto compliance is certain. With millions of crypto transactions taking place each day, crypto compliance will become an absolute necessity.

Further, the sectors within the crypto industry that will require crypto compliance will continue to grow as novel applications for the blockchain increase. For example, certain types of non-fungible tokens (NFTs) may find themselves in the crosshairs of government regulators. Specifically, the U.S. Commodity Futures Trading Commission (CFTC) may find certain types of contracts for the future delivery of an NFT or the terms and structure of an NFT contract subject to application of the Commodity Exchange Act or the Dodd-Frank Act, or the U.S. Securities and Exchange

Commission (SEC) might find that fractionalized NFTs qualify as securities.

Crypto compliance will also be required on a global scale. On June 21, 2021, the Financial Action Task Force (FATF) issued guidance for its member states, which includes thirty-seven member jurisdictions, two regional organizations, and multiple associate members and observing organizations, recommending that they implement and ensure compliance with Know Your Customer (KYC) and AML protocols[4]. FATF further recommended that its members states engage in international cooperation in this area of compliance to combat money laundering and the financing of terrorism. FATF has also announced its plans to develop standards and guidance for regulating peer-to-peer (P2P) transactions[5].

Lastly, the longer parts of crypto continue to exist in legal and regulatory gray areas (e.g., some decentralized finance (DeFi) projects), the more likely lawmakers and regulators are to target these companies with new laws and regulations or attempt to bring them under the current regulatory frameworks. These moves will result in the continued growth and application of crypto compliance in the crypto industry.

4. FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, https://www.fatf-gafi.org/recommendations.html (Updated June 21, 2021)
5. FATF, Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html (June 21, 2021).

Chapter 2:
The Big Three Considerations of Crypto Compliance

Today, a myriad of considerations must be considered for effective crypto compliance, such as business registration, sales regulations, securities laws, money transmission laws, tax treatment, business licensing, anti-money laundering protocols, mining regulations, and custody of funds.

This chapter elaborates on the three most important considerations in crypto compliance.

Anti-Money Laundering Compliance

In its most basic form, AML Compliance is defined as:

“The policies and procedures implemented and followed to detect, prevent, and combat money laundering, terrorism financing, and other financial crimes.”

However, AML compliance is more than this, especially in the world of crypto compliance, and while each country has its own AML rules and regulations, FATF has a list of 40 recommendations that each country should follow. In the U.S., the Financial Crimes Enforcement Network (FinCEN) enforces the BSA and AML compliance.

AML Protocols

In the U.S., AML compliance requires, among other things, that a business have a written risk based anti-money laundering program approved by senior management. The AML program must include, at a minimum:

1. the establishment and implementation of policies, procedures, and internal controls reasonably designed to prevent money laundering or the financing of terrorist activities and to achieve compliance with the BSA and implementing regulations;
2. independent testing for compliance;
3. designation of an individual or individuals responsible for implementing and monitoring the operations and internal controls of the program;
4. ongoing training of appropriate personnel; and
5. appropriate risk-based procedures for conducting ongoing customer due diligence, including, but not limited to, understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile, and conducting ongoing monitoring to identify and report suspicious transactions.

Know Your Customer (KYC)

KYC is a process to ensure the legitimacy of customers by verifying their identity for risk assessment. It is a part of the AML compliance process to prevent fraudulent activities and financial crimes.

Crypto services providers, including, among others, hosted crypto wallet providers and crypto exchanges, that fall under the definition of MSBs or “money transmitters” provided by FinCEN, must become KYC compliant to operate.

There are three steps for an effective KYC process:

1. Customer identification;
2. Customer due diligence; and
3. Persistent monitoring.

Within that framework, there are levels of due diligence that may be required:

- ✓ Simplified customer due diligence;
- ✓ Standard customer due diligence; and
- ✓ Enhanced customer due diligence.

This framework properly identifies a customer, allows a customer risk profile to be created, and ensures that suspicious activity is identified and reported.

Suspicious Transactions

In 2020, FATF released a report to help crypto exchanges and crypto wallet providers in developing their AML programs to identify suspicious transactions[6]. The report included guidance to identify suspicious:

- ✓ Transaction types;
- ✓ Transaction patterns;
- ✓ Anonymity;
- ✓ Senders and recipients;
- ✓ Source of funds;
- ✓ Geographical risks.

6. FATF, Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets, www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html (Sept. 2020).

Registration with FinCEN

The Financial Crimes Enforcement Network (FinCEN) is a bureau of the United States Department of the Treasury that collects and analyzes information about financial transactions to combat money laundering, terrorist financing, and other financial crimes.

FinCEN registration, reporting, and recordkeeping is mandatory for all money services businesses (MSBs) unless a limitation or exemption applies. An MSB must register within 180 days of being established and renew its registration every two years. MSBs include people and businesses involved in the transmission of virtual currencies[7]. With FinCEN registration, you are informing FinCEN about your type of business, who owns the business, and where you conduct your business.

The following sections explain how FinCEN regulations apply to certain types of crypto MSBs under BSA/AML rules and regulations.

Obligations of Crypto Transmitters

FinCEN, under BSA/AML regulations, requires crypto transmitters to develop, implement, and maintain the AML Protocols discussed in the previous section. Namely, this includes having a written AML program to prevent the facilitation of money laundering and financing of terrorist activities. The program should be submitted to independent testing to ensure compliance with BSA/AML requirements and to ensure the overall efficacy of the compliance program.

7. See FinCEN 2013 Guidance.

Crypto transmitters are also obligated to incorporate policies, procedures, and internal controls to ensure ongoing compliance by verifying customer identification (KYC procedures), creating and retaining records, filing reports, and responding to law enforcement requests.

Lastly, a designated individual must ensure day-to-day BSA/AML compliance and provide training to personnel for the detection of suspicious activity.

Guidance for Business Models involving Crypto

This section includes guidance for regarding the regulatory status of specific business models dealing with crypto transactions. This guidance does not include an analysis or discussion of the state-by-state money transmitter requirements that some crypto companies must comply with, so you should check your state's laws on these topics.

P2P Exchangers

All exchangers are in the business of accepting a convertible virtual currency and transmitting it to another person or place are required to comply with BSA/AML regulations and register with FinCEN as an MSB, regardless of the location from which they are operating if they are doing business wholly or in substantial part within the U.S.

Crypto Wallets

FinCEN's guidance for crypto wallets applies to mobile wallets, software wallets, and hardware wallets.

Hosted (Custodial)/Unhosted (Non-custodial) Wallet Providers

In the case of transactions from hosted wallets, the host must follow the AML procedures outlined for identifying, verifying, and monitoring the user's identity and transactions, as well as ensuring proper recordkeeping and reporting. This obligations results from accepting possession of and transmitting a virtual currency.

Currently, in the case of transactions from single-signature, unhosted wallets (e.g., a crypto wallet on a person's computer, phone, or a similar device), FinCEN does not label them as money transmissions because the user retains full control over the virtual currency. The wallet provider simply provides software to the user[8].

Multiple-Signature Wallets Providers

If multisig wallet providers provide unhosted wallets to users, the providers are not money transmitters under the BSA.

If multisig wallet providers provide hosted wallets, they qualify as money transmitters, and all of the compliance obligations that apply to crypto transmitters apply to them. Thus, they must comply with BSA/AML regulations and register with FinCEN.

Kiosks

Kiosks are more commonly known as Crypto ATMs or Bitcoin ATMs.

An owner operator of Kiosks that accept and transmit crypto (i.e., acts as a third-party exchanger) qualifies as a money

8. U.S. Dep't of the Treasury, Fin. Crimes Enf't Network, FIN-2014-R002, Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity (Jan. 30, 2014) (stating that "providing software, in and of itself, does not constitute acceptance and transmission of value, even if the purpose of the software is to facilitate the sale of virtual currency").

transmitter, and all of the obligations that apply to crypto transmitters apply to the owner operator. Thus, they must comply with BSA/AML regulations and register with FinCEN.

An owner operator of Kiosks that only verifies balances and dispenses currency as a sale or purchase by the owner operator directly with the customer is not classified as a money transmitter under the BSA.

DApps

Decentralized applications (DApp) fall under the same umbrella as Kiosks (i.e., mechanical agencies). All regulations and compliance requirements that apply to Kiosks, apply to DApps and their owners operators.

Anonymity Enhanced Transactions

A crypto transmitter that operates in anonymity-enhanced crypto is subject to the same regulatory and compliance obligations as when operating in non-anonymized crypto.

A money transmitter cannot avoid its regulatory and compliance obligations by operating in anonymity-enhanced crypto.

Crypto Payment Processing Services

Crypto payment processing services allow traditional merchants to sell their goods in exchange for cryptocurrency. Such payment processors fall within the definition of money transmitters and are bound by the regulatory and compliance obligations put forth by FinCEN under BSA/AML regulations.

Crypto Licensing

Licenses are an absolute requirement to set up and operate a crypto exchange, and licensing procedures heavily depend on the locations in which the exchange is going to operate. Different jurisdictions often offer several different licenses including licenses for crypto exchanges and operating crypto wallets.

Global Licenses

Although there are several licensing authorities around the world, this section discusses the 3 major license providers in different parts of the world.

Swiss FINMA License

In 2019, the Swiss Financial Market Supervisory Authority (FINMA) together with the Swiss State Secretariat for International Finance (SIF) implemented a FinTech license. The license applies to crypto services that fall under Switzerland's laws and regulations governing banking and securities.

UK FCA License

In 2020, the Financial Conduct Authority (FCA) officially became the anti-money laundering and counter terrorist financing supervisor for crypto-related activities in the UK. The FCA regulations and registration requirement generally target and require the following types of businesses to register with the FCA[9]:

1. Businesses that exchange, or arrange or make arrangements with a view to exchange cryptoassets for money or vice versa, or one cryptoasset for another cryptoasset;

9. See Regulation 14A of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, as amended.

2 Businesses that operate a machine which uses automated processes to exchange money for cryptoassets or vice versa (e.g., an ATM);

3 Businesses that provide custodian services for (i) cryptoassets on behalf of customers or (ii) private cryptographic keys to hold, store and transfer cryptoassets.

Estonia FIU License

In Estonia, the Financial Intelligence Unit (FIU) provides two different licenses for crypto service providers: licenses for services providers who exchange a virtual currency against a fiat currency and crypto wallet providers.

Chapter 3: Levels of Regulations and Compliance Around The World

Local Compliance

In the U.S., rules and regulations around crypto differ widely from state to state but the basics of compliance can generally be derived from the guidelines provided by FinCEN, under its application of BSA/AML regulations, and the Office of Foreign Assets Control (OFAC), under its power to enforce economic and trade sanctions.

Regional Compliance

Although compliance differs widely from country to country, most regions have laws and regulations in place that are common throughout the region. This section presents the commonalities and differences in compliance for regions around the world.

Africa

In most African countries, cryptocurrencies are not recognized as currencies in circulation. Outliers in Africa include Mauritius and South Africa, where South Africa is the closest country to putting cryptocurrencies in a legal framework and by extension implementing strict rules and regulations for compliance. Specifically, South Africa is currently focusing on establishing AML and KYC protocols for crypto exchanges after multiple crypto scams within the country.

On the other hand, a few African countries including Morocco, Algeria, and Libya have banned cryptocurrencies altogether.

Americas

The regulation and rules of compliance in the Americas differ between countries, states, and government entities.

In North American countries, cryptocurrencies are not recognized as legal tender but an extensive set of rules and regulations governing the crypto industry exist. For instance, in Canada, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) facilitates the detection, prevention, and deterrence of money laundering and the financing of terrorist activities under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its associated regulations.

In South America, the situation is quite the opposite, as countries have taken varying approaches to regulating crypto. For instance, Bolivia has banned any decentralized cryptocurrency, while El Salvador and Venezuela have either adopted bitcoin or their own virtual currency as legal tender. Additionally, a working committee for the regulation of crypto has been established in Brazil, and Columbia is carrying out studies to implement taxes on cryptocurrencies.

Asia

A major portion of all crypto transactions derive from Asia. However, treatment of crypto in the region varies greatly.

In Japan, cryptocurrencies are recognized as legal tender and are regulated under the Payment Services Act (PSA) and Financial Instruments and Exchange Act. Japan’s Financial

Services Agency has also certified two self-regulatory groups as Certified Financial Instruments and Exchange Associations. One such group, the Japan Crypto Asset Trading Business Association, formerly the Japan Virtual Currency Exchange Business Association, is the official self-regulating organization for crypto in Japan. This group is authorized to create and enforce regulations for crypto exchanges in Japan.

In China, the government has banned cryptocurrencies and crypto mining entirely. However, the Central Bank of China has established a “Digital Money Institute” to issue its own digital currency.

In South Korea, rules and regulations are in place to ensure that cryptocurrencies are processed only through registered financial institutions like banks. Crypto trading with anonymous bank accounts is strictly prohibited.

In Singapore, crypto activities, including ICOs, are regulated by the Monetary Authority of Singapore (MAS) under their Capital Market Law.

In Malaysia, digital asset platforms must be compliant with and approved by the Securities Commission. ICO activities cannot be carried out unless approved by the Securities Commission.

In Thailand, digital assets and cryptocurrencies are regulated separately under two different frameworks for taxes on transactions and income derived from transactions. Lately, the Thai SEC has been actively regulating the crypto industry and has warned against DeFi operations and banned “meme” tokens and NFT trading.

Europe

For countries within the European Union, only certain categories of crypto service providers fall under the EU's Money Laundering Directives. However, reform proposals to extend the rules to the entire crypto industry have been put forth.

Australia

In Australia, the use, trade, and mining activities of crypto are legal, but certain activities are subject to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF 2006), section 5 and associated rules. The crypto industry in Australia is predominantly regulated by the Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Australian Securities and Investment Commission (ASIC). These agencies regulate exchange registration requirements and the conditions in which ICOs are evaluated as financial transactions.

Bank-Grade Compliance

Bank-Grade Compliance is a relatively new term coined by Elliptic to represent a level of compliance that is equal to the compliance requirements mandated for traditional financial institutions.

Bank-Grade compliance is the highest level of compliance.

Chapter 4:
Pitfalls of Non-Compliance

The pitfalls of non-compliance include imprisonment, financial penalties, and reputational and productivity loss. The mere announcement of a civil fine or regulatory action can decrease the market value of a crypto company or the cryptoasset being targeted. In the long run, non-compliance costs far more than compliance.

Non-Compliance with U.S. Securities Laws

Non-compliance with the Securities Act of 1933 and the Securities Act of 1934, and their corresponding regulations, as enforced by the SEC, can result in fines, settlements, restraining orders, cease-and-desists, asset freezes, and district court actions. While the SEC lacks criminal authority, it can refer matters to a state or federal prosecutor to pursue a criminal action.

Case Studies of Non-Compliance

Settlements

In 2021, the SEC settled charges against:

- ✓ Poloniex, LLC., under which Poloniex agreed to pay more than $10 million, for operating an unregistered online digital asset exchange.
- ✓ Uulala, Inc., under which Uulala agreed to pay more than $9 million and disable its tokens, for defrauding more than a thousand investors in an unregistered offering of digital asset securities.

- Loci, Inc., under which Loci agreed to pay $7.6 million and disable its tokens, for making materially false and misleading statements in connection with an unregistered offer and sale of digital asset securities.

Restraining Order

In 2021, the SEC filed an emergency action and obtained a restraining order against:

- Shawn C. Cutting, for raising millions of dollars from hundreds of investors by falsely claiming to be a financial adviser with securities licenses, overstating investment returns, and misappropriating money received from investors.
- Sean Hvizdzak, Shane Hvizdzak and three entities they controlled to stop an offering fraud and the misappropriation of investor proceeds.

Cease-and-Desist

In 2020-2021, the SEC filed a settled cease-and-desist proceeding against:

- Wireline, Inc., for offering and selling unregistered securities in the form of investment contracts when it offered and sold digital assets through simple agreements for future tokens and for making materially false and misleading statements in connection with an unregistered offer and sale of digital asset securities.
- Tierion, Inc., under which Tierion returned funds to harmed investors, paid a $250,000 penalty, and disable trading in its “tokens,” for conducting an unregistered offering of securities in the form of a “token sale.”

- ShipChain, Inc., for raising funds through an unregistered initial coin offering of digital tokens.

Asset Freeze

In 2020, the SEC filed an emergency action and obtained an order for an asset freeze against:

- Virgil Capital LLC, for securities fraud related to their flagship cryptocurrency trading fund.
- Daniel F. Putman, Jean Paul Ramirez Rico, and Angel A. Rodriguez, for defrauding investors out of more than $12 million in two cryptocurrency-related schemes.

District Court Action

In 2019, the SEC filed a settled district court action against:

- Eran Eyal, founder of UnitedData, Inc. d/b/a Shopin, seeking permanent injunctions, disgorgement with interest, and civil penalties, as well as an officer-and-director bar against Eyal and a bar against Eyal and Shopin prohibiting them from participating in any future offering of digital-asset securities following a fraudulent unregistered securities offering by selling tokens in an ICO.

Non-Compliance with BSA/AML

Non-compliance with the BSA and AML requirements, as enforced by FinCEN, can result in imprisonment, financial penalties, warning letters, orders to comply, public naming, suspension or revocation of license or registration, prohibiting individuals from operating in financial services, and removing, restricting, replacing, or restricting the powers of managers, directors, and controlling owners.

Case Studies of Non-Compliance

In 2021, FinCEN sought enforcement for non-compliance with BSA/AML regulations against:

- BitMEX, under which FinCEN assessed a civil money penalty in the amount of $100 million, for operating as an unregistered “futures commission merchant” in violation of the Commodity Exchange Act (CEA) and for providing money transmission services, transmitting funds for U.S. Customers by accepting currency, funds, or other value that substitutes for currency from one person and transmitting currency, funds, or other value that substitutes for currency to another location or person.

In 2019 FinCEN sought enforcement for non-compliance with BSA/AML regulations against:

- Eric Powers, under which FinCEN assessed a civil money penalty in the amount of $35,000, for willfully violated the BSA by failing to (i) register as a money services business (MSB), (ii) implement written policies and procedures for ensuring BSA compliance, and (iii) report suspicious transactions and currency transactions.

In 2017, FinCEN sought enforcement for non-compliance with BSA/AML regulations against:

- Larry Dean Harmon, the founder of Coin Ninja, was fined $60 million for violations of the BSA and its implementing regulations on charges of conspiracy to launder monetary instruments and the operation of an unlicensed money transmitting business .

Conclusion

Becoming compliant with FinCEN and BSA/AML laws and regulations is not an easy task, and it can cost a fair amount of effort and resources. However, the repercussions of non-compliance are far greater.

For this reason, it is important to go through all the rules and regulations of the state, country, or region where your organization operates.

For a smooth compliance process, follow these best practices:

Non-Compliance with BSA/AML

- ✓ Stay up to date with the rules and regulations put forth by the SEC and FinCEN.
- ✓ Consult a crypto compliance expert or agency before offering any form of crypto service.
- ✓ Register with FinCEN.
- ✓ Get licensed before actively operating your crypto business.
- ✓ Hire a professional to ensure continuous compliance.
- ✓ Create a written AML program and make sure that it is implemented.
- ✓ Train your staff to identify crypto frauds and non-compliance.
- ✓ Engage in customer due diligence.

Properly record and report suspicious activity.