Compliance for Digital Assets: Best Practices you need to know[1]

Neepa Patel, Chief Compliance Officer at R3

Regulatory Guidelines for Wallet Providers, Virtual Asset Service Providers and Digital Asset Issuers[2]

Thinking about issuing a stablecoin or security token (collectively referred to as a "digital asset")? Make sure to read these guidelines first. There is widespread recognition of the need for adequate and consistent measures to deploy tokens in the cryptocurrency space. The creation of laws without global coordination may give rise to a fragmented regulatory landscape. While regulators have yet to catch up with cryptocurrency innovations, criminals have abused them and left legitimate users vulnerable to theft, fraud, and other risks. Please note that the following recommendations are only suggestions and should not be viewed as conclusive or exhaustive.

Regulations / Regulatory Entity	Applicability for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers	Compliance Recommendations for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers
Know Your Customer (KYC)/ Anti-Money Laundering • **Global standards to verify the identity of customers (individuals and legal entities), and assess their risks of engaging in illicit activity.** *Applies to Issuers of Stablecoins and Digital Securities, Exchanges, MSB and Wallet Providers.*	• **Identity verifications cover initial onboarding and ongoing checks of customers.** • **Customer Due Diligence (CDD) requires identity documentation to evaluate the risk profile of a customer.** • **Enhanced Due Diligence (EDD) refers to more detailed verifications and additional documentation for higher risk customers.** • **Latest CDD Rule of 2018 requires information about beneficial owners who control or own at least 25% of a legal entity** • **Watch list screening refers to ensuring customers do not belong to sanctions lists, terrorist lists, etc.**	• **Periodically update KYC information on accounts conducting large volume trades and frequent transactions.** • **Perform enhanced due diligence[3] on higher risk customers and customers transacting in larger quantities.** • **For large volume deposits and transfers, understand the source of funding.** • **Document reasons for denying customers (e.g. do not meet accredited investor rules, sanctioned, high risk etc.).** • **Properly investigate exceptions and maintain supporting documentation.**

[1] The information provided in this report does not, and is not intended to, constitute legal advice. All information, content, materials, charts, and graphs contained in this report are for general informational purposes only. Links contained in the report are for the convenience of the reader; R3 LLC, its members, and its affiliates do not recommend or endorse the contents of the third-party sites. Readers of this report should contact their attorney to obtain advice with respect to any particular matter.

[2] The following information is for general informational purposes only and should not be relied upon as an exhaustive survey of the applicable laws associated with stablecoin and/or digital token issuers.

[3] Enhanced due diligence (EDD) for higher-risk customers is especially critical in understanding their anticipated transactions and implementing a suspicious activity monitoring system that reduces the bank's reputation, compliance, and transaction risks. Higher-risk customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the bank.

Regulations / Regulatory Entity	Applicability for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers	Compliance Recommendations for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers
	• Transaction monitoring refers to observing and detecting patterns of activity in order to identify suspicious behavior. • Customer Identification Program (CIP) refers to a USA PATRIOT Act provision requiring financial institutions to verify the identity of individuals they transact with by obtaining name, address, DOB and unique ID.	
Bank Secrecy Act (BSA) • Primary US anti-money laundering (AML) law. • Amended by the USA PATRIOT Act of 2001, requiring financial institutions to enforce specific AML compliance programs. • Similar rules apply to SEC / CFTC governed institutions. *Applies to Issuers of Stablecoins and Digital Securities, Exchanges, Wallet Providers and MSBs operating in the US.*	• Notable concerns around potential anonymity, the fact that crypto currencies can be accessed from virtually anywhere in the world, the ease of transfers internationally and the lack of transaction limits. • May 9th, 2018 FinCEN Advisory requires P2P exchangers, including foreign located businesses operating in the US, to register as an MSB and comply with BSA rules.	• Enforce AML/BSA compliance programs accordingly (set written internal policies/ procedures/controls; appoint experienced compliance officers; ongoing AML training for employees; independent testing of compliance programs).
Office of Foreign Asset Control (OFAC) / Sanctions • A restriction to transact with specific countries / individuals on a government issued blacklist. *Applies to Issuers of Stablecoins and Digital Securities, Exchanges, Wallet Providers and MSBs with US clients.*	• Virtual Asset Service Providers must conduct sanction screens on clients and prevent token transfers to wallets blacklisted internally and externally.	• Establish proper controls to prevent stablecoin and digital securities transfers to Blacklisted Digital Wallet Addresses. Depending on the jurisdiction, multiple sanction lists must be used. • Screen customers periodically, if not daily, against updated sanctions lists.

Regulations / Regulatory Entity	Applicability for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers	Compliance Recommendations for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers
Financial Crimes Enforcement Network (FinCEN) • US Treasury Department bureau collecting and analyzing data on financial transactions to combat money laundering, terrorist financing, and other financial crimes. • Shares information and coordinates with foreign financial intelligence (FIU) counterparts on AML efforts. • May 9th, 2018 FinCEN Advisory requires P2P exchangers, including foreign located businesses operating in the US, to register as an MSB and comply with BSA rules. *Applies to any entity engaging in money transmission in the U.S. with respect to convertible virtual currency, including Exchanges and Wallet Providers.*	• Expected clarification on the applicability of BSA regulations to create, obtain, distribute, exchange, accept, and transmit virtual currencies. • Entities engaging in virtual currency transactions fall under the Money Service Business (MSB) Rule, which updates MSB regulations for foreign exchange and money transmitting services. • Real currency defined as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance." • Virtual currency defined as "medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency" like legal tender • Convertible virtual currency defined as having an equivalent real currency value, and can substitute a real currency.	• File suspicious activity reports (SAR) within 30 days of identifying suspicious activity. • Re-evaluate relationships with exchanges and customers that result in multiple SAR filings. • Investigate activity by utilizing AML tools, detecting patterns / trends in account activity and researching customer social media activity. • Stay current on sophisticated money laundering techniques and make improvements to AML detection systems. • Provide continuous training to AML staff on new and sophisticated techniques used by money launderers.

Regulations / Regulatory Entity	Applicability for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers	Compliance Recommendations for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers
Consumer Complaints (US) • Consumers can submit complaints to the Consumer Financial Protection Bureau (CFPB) for financial related products and services. Institutions must reply to customer complaints within 15 days. • Consumers can also file complaints with the FTC or their state Attorney General regarding issues with consumer products or services, potentially including stablecoins or digital assets *Applies to Issuers of Stablecoins and Digital Securities, Exchanges, Wallet Providers, and technology providers.*	• No central agency exists to monitor complaints for token issuers. • Complaints can assist token issuers to revise internal processes and help improve issuer reputation.	• Allow customers to escalate complaints to digital token issuer via website link or other means. • Respond to customer complaints within 30 days or a set time frame and keep documented records of complaint date, response and responder for audit purposes.
Conflict of Interest • A situation that can unfairly harm investors from missing or incomplete disclosures. *Applies to Issuers of Stablecoins and Digital Securities, Exchanges, Wallet Providers, and technology providers*	• Conflicts of interest with respect to securities are usually disclosed in offering Memorandums or private placement memos. • No person/entity associated with a broker dealer shall accept any payment (directly or indirectly) from an issuer of a security for publishing a quotation.	• Crypto exchange employees involved with listing new tokens on exchanges should refrain from trading on non-public information. • Traders should disclose conflicts they may have when executing or having visibility to client trades. • Disclose material holders of digital assets and publicly disclose names of large holders who can move markets. • Exchanges participating in proprietary trading should have “Chinese Wall” controls in place.

Regulations / Regulatory Entity	Applicability for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers	Compliance Recommendations for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers
Financial Act Task Force (FATF) • Global standard-setter for anti-money laundering/ counter-terrorism financing (AML/CTF) regulation. • 2015 guidance encouraged countries to regulate exchange services between fiat and virtual currencies, without the desired results. *Applies to Issuers of Stablecoins and Digital Securities, Exchanges, Wallet Providers, and technology providers.*	• Proposed rules that Virtual Asset Providers (VASPs) may be required to obtain, hold and transmit both originator and benificiary information. • Emphasis on urgent need for a coordinated international approach to inhibit criminal and terrorist uses of virtual assets. • More robust regulation of virtual assets: expanding the scope of existing regulatory regimes, and censuring countries not taking sufficient measures. • Oversight expected to extend beyond fiat-to-virtual currency conversions, to include virtual-to-virtual currency conversions and related services. • Expanding scope of entities subject to existing AML/CFT regulations.	• Identify opportunities to share information on suspicious transactions with global agencies and competitors while keeping privacy intact. • Set compliance measures to meet various international cryptocurrency standards.
US Travel Rule and EU Transfer Rule: • Applies to a transfer of funds, in any currency. Specific information required for payments above a specific threshold. *Wallet providers and exchanges*	• Travel rule regulations require specific fields including the originator and beneficiary to be known. • Due to the design of public blockchains and the inconsistency of regulatory implementation amongst wallet providers, it is difficult to attach human readable identity information between wallets.	• Research advanced techniques utilizing cryptography and encryption that may address the original intent of the travel rule without sending human readable information. • Build relationships with exchanges and wallet providers with strong KYC / AML processes to minimize the risk of digital token transfers to fraudulent parties.

Regulations / Regulatory Entity	Applicability for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers	Compliance Recommendations for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers
Fifth Anti-Money Laundering Directive (AMLD5) • Enforced by the European Parliament, as the European Union's most comprehensive set of AML regulations. • Passed as the implementation of FATF recommendations. *Applies to Virtual Currency Platforms, exchanges and wallet providers.*	• Fifth iteration after AMLD4 expands the scope of AML regulations to cryptocurrencies. • Intended to bring crypto measures in line with US regulations, and a key step toward harmonizing cryptocurrency regulations and reducing regulatory arbitrage for criminal activity. • Specifically covers exchanges between fiat and virtual currencies and custodian wallet providers that hold users' private keys. • Formalizes AML/CTF and KYC requirements for crypto businesses, including CDD and transaction monitoring. • EU-wide adoption expected by the end of 2019.	• Conduct ongoing monitoring of relationships and report suspicious activity to government entities. • Research opportunities to work with other foreign VASPs to register users' identities and wallet addresses while preserving privacy/GDPR.
Markets in Financial Instruments Directive (MiFID II) • EU legislative framework for financial markets, to improve investor protection, reporting requirements, and restoring confidence after the 2008 financial crisis. *Applies to Digital Security issuers.*	• European Securities Market Authority (ESMA) advised to the European Commission, Council, and Parliament that all crypto platforms that trade crypto assets qualifying as financial instruments must comply with MiFID II rules. • MiFID II rules cover certain crypto asset trading platforms with central books and/or matching orders (multilateral trading platforms) and entities executing client orders with proprietary capital (broker dealers) (3 categories).	• Ensure disclosures to investors are fair and accurate. Inform investors of potential risks. • Depending on the underlying asset, determine if MiFID II would trigger regulatory reporting requirements.

Regulations / Regulatory Entity	Applicability for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers	Compliance Recommendations for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers
	• All EU regulations apply to crypto assets that qualify as financial instruments. • Expected efforts to tailor EU rules to address risks and issues pertaining to crypto assets and asset tokens, such as the definition of "transferrable securities," "commodities," and the MiFID list of "financial instruments". • Expected reconsideration of required pre- and post-trade transparency measures, transaction and trade reporting could apply to crypto assets identified as securities.	
General Data Protection Regulation (GDPR) • EU legislation to safeguard protection of personal data and privacy, and give individuals greater control over their information. *Applies to Stablecoin and Digital Securities issuers, exchanges, virtual currency platforms, technology companies and wallet providers.*	• Requirement for business processes to integrate policies and practices to keep data private, process it with individuals' consent, and withdraw it at any time upon individuals' request. • Processing of personal data must have a lawful basis, and individuals' consent must be freely given, specific, informed, and unambiguous. • Individuals and data subjects are in charge of their own data and have a right to use it across institutions, a right to withdraw it and make it "forgotten", and a right to be informed about breaches impacting their rights and freedoms.	• Store personal data in secure databases with limited employee accessibility. • Allow customers to amend or update personal data when it is inaccurate. • Maintain an inventory of all systems housing personal data – internal and external - and assign a system owner responsible for deleting data after record retention rules expire.

Regulations / Regulatory Entity	Applicability for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers	Compliance Recommendations for Wallet Providers / Virtual Asset Service Providers / Digital Asset Issuers
Concentration Risk and Vendor Due Diligence • **Risk arising from concentration to a single counterparty, sector or country.** *Applies to Stablecoin and Digital Securities issuers, exchanges, virtual currency platforms, technology companies and wallet providers.*	• **Cybersecurity risk from custodial wallet providers or other centralized trading platforms that hold private keys on behalf of their clients and have been subject to cyber incidents** • **Financial, Operational, Privacy and IT Risk associated with 3rd party vendors used by wallet providers, token issuers and exchanges.**	• **Obtain independent platform audits such as SOC 2 or ISO 27001.** • **Periodically test disaster recovery & BCP plans to ensure controls are in place to address cyber incidents.** • **Complete comprehensive Risk Assessments and vendor due diligence to analyze risk associated with vendors and strategic partners involved with company operations or confidential information.** • **Engage external auditors to verify custodian collateral is consistent with on-ledger amounts.**
Foreign Account Tax Compliance Act (FATCA) • **Financial assets equivalent to $10,000 held by US investors abroad must be reported to the US tax authority.** • **The US has Intergovernmental Agreements in place with certain jurisdictions.** *Applies to exchanges and virtual currency converters*	• **If you are a US investor who purchased cryptocurrency on a non-US exchange, you might be subject to FATCA.** • **The exchange platform does not have to have a banking license to fall in scope.** • **A foreign crypto exchange may have to report US investors under FATCA to the IRS and a foreign investor with a US exchange account may have to report activity to a foreign jurisdiction tax authority.**	• **Comply with FATCA and have documentation available on user account balances if approached by a government agency, including the IRS.**

Source: Author and R3: **Will Businesses Ever Use Stablecoins**

External Audits

With the myriad of scandals plaguing the digital token industry, conducting an external audit by an independent party can instill public confidence in your offering. Fiat and other asset reserves, nevertheless, can be a clear indication of solvency. Applicability of AML rules to fiat-pegged assets should be commensurate to payment rules, but AML rules may still be unclear when dealing with non-fiat assets.

One challenge today is that there are no audit standards for digital tokens – fiat backed and non-fiat backed – to confirm their issuers' solvency. This is made more complex when collateral is held by multiple fragmented entities. When developing standards, auditors should ensure the following business processes are reviewed:

RESERVE RECONCILIATION	Attest that the value of assets held in custody accounts exceeds the balance of tokens issued on a blockchain.
INTERNAL CONTROLS	Review issuance and redemption controls to ensure proper segregation of duties, four eye checks and controls to prevent hacking are in place. Ensure processes are documented and access to sensitive information is limited.
AML / KYC FRAMEWORK	Review KYC documentation. Controls related to enhanced due diligence, the exception monitoring process and denied account documentation should be reviewed.
PRIVACY / RECORD RETENTION	Safekeeping client information and disposing all information after record retention rules expire. Review controls around personal data and customer access to ensure GDPR compliance.
MARKETING AND ADVERTISING	Whitepapers and periodic reports must include fair and accurate information and potential risks to investors. Proper disclosures should be placed on all external correspondence and marketing strategy should be consistent with SEC filing documents (if required).

Source: R3

Digital Asset issuers should make material audit findings public.

Applicable Licenses – Stablecoins

Stablecoin issuers may fall under the following licenses, regardless of whether they currently hold them officially. These licenses are not all mutually exclusive and can be acquired in combination. But because there is little clarity as to which licenses stablecoin issuers are required to comply with, issuers have thus far adopted them in fragmented ways.

Trust	A stablecoin issuer may pursue a trust structure, in which the trust administers financial assets on behalf of stablecoin users. Taking the role of a fiduciary, an issuer typically commits to managing, recording, monitoring, and safeguarding the assets under its control. Several stablecoin issuers have acquired state-issued limited purpose trust company charters, which are designated for specific trust functions such as depositing and safekeeping assets. Responsibilities for cryptocurrency activities remain open-ended. Trust company status alone may be insufficient to ensure adequate governance.
Money Service Business Registration and Licensing	MSBs must be registered at the federal level and MSBs that are money transmitters must be licensed at the state level. MSBs must comply with the Bank Secrecy Act ("BSA") and the related rules, which impose significant KYC and anti-money laundering (AML) obligations. Generally, money transmitters engage in activities as administrators or exchangers. Stablecoin issuers fall under the category of virtual currency "exchangers," managing conversions from fiat to stablecoin, crypto to stablecoin, etc. They are also virtual currency "administrators" by issuing and redeeming coins, placing and withdrawing them from circulation. Operating as "money transmitters,"[4] they are subject to MSB standards for registration, reporting, and recordkeeping.
Regional Licensing	Depending on their intended uses and jurisdictions, stablecoin issuers may pursue licenses for specific lines of activity (US money transmission licenses, EU e-money transmission licenses, international company licenses, etc.). Yet these may be limited in scope in relation to overall stablecoin operations and may be implemented in fragmented ways. Moreover, if these licenses are not designed for cryptocurrencies, their applicability to stablecoins may require additional interpretation.
Bitlicense	A business license for virtual currency business activities involving New York state or its residents, issued by the New York State Department of Financial Services. BitLicenses clearly specify compliance for activities defined as receiving and transmitting virtual currencies; storing, holding, and maintaining custody or control on behalf of others; buying and selling virtual currencies; exchange services; and controlling, administering, or issuing virtual currencies. While the exact numbers are unclear, as of June 2019, it is estimated that 20 BitLicenses have been granted to entities globally.

Source: R3: **Will Businesses Ever Use Stablecion**

[4] "An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person."

Reg A (+)

Established companies raising capital for growth

Offering must be qualified by the staff at the SEC

- Available to issuers with a principal place of business in the U.S. or Canada
- Not available to companies required to register under the Investment Company Act of 1940 or Business Development Companies
- Not available to development stage companies
- Solicitations of interest in compliance with rules permitted
- Ongoing reporting obligations
- Bad actor disqualification

Tier 1:

- Investment up to $20 million in a 12-month period
- File a Form 1-Z exit report upon termination or completion of offering
- Subject to registration or qualification in any state in which securities will be offered for sale

Tier 2:

- Investment up to $50 million in a 12-month period
- Can list on securities exchange
- Limitations on non-accredited investors
- File annual and semiannual reports, as well as current reports upon the occurrence of certain events. Possible obligation to file exit report.
- Exempt from state securities laws except for anti-fraud.

Reg S

Safe harbor from the registration requirements of the federal securities laws

- Applies to offshore offers to non-U.S. persons
- Directed selling efforts prohibited
  - Activity that might condition the U.S. market for flowback of securities
- Offer will be subject to additional conditions depending on categorization
- Category 1
  - Foreign Issuers
    - No substantial U.S. market interest (SUSMI), or
    - Overseas directed offering
  - No additional conditions
- Category 2
  - Equity securities of a foreign issuer
  - Debt securities of a foreign or a reporting U.S. issuer.
  - 40-day distribution compliance period
- Category 3
  - Debt of non-reporting US issuers
    - 40 day distribution compliance period
  - Equity offerings by U.S. reporting issuers
    - 6-month distribution compliance period
  - Equity offerings by non-reporting U.S. issuers or foreign issuers for which there is SUSMI
    - 12-month distribution compliance period

Source: DLx Law

Reg D – Form D

Smaller companies to raise capital via debt/ equity sales

- **Reg D Rule 504**
  - **$5 million limit in 12-mth period**
  - **Holding period 6mth – 1 yr w/o registering**
- **Reg D Rule 506(b)**
  - **Accredited investors & up to 35 non-accredited investors**
  - **No limit on amount raised or investment per investor**
  - **No general solicitation**
- **Reg D Rule 506(c)**
  - **Only accredited investors**
  - **No limit on amount raised**
  - **General solicitation permitted**
  - **Verification of accredited status required**

Reg CF

Crowdfunding

- **U.S. companies only and other eligibility restriction**
- **Offering must be listed on a registered funding portal or broker**
- **Public communication / advertising limited**
- **Issuers may not raise more than $1,070,000 million in any 12-month period**
- **Amounts sold in other exempt offerings during the preceding 12-month period are not aggregated.**
- **Investor limitations depend on annual income / net worth**
- **Disclosure requirements – Form C**

Source: DLx Law

Continue the conversation

r3.com

@inside_r3

medium.com/inside-r3

R3 Author

Neepa Patel, Chief Compliance Officer, R3

R3 Contributors

DLx Law and Diane Barrero Zalles

About this publication

This publication is intended for informational and educational purposes only and does not replace independent professional judgment or advice. No information contained in this publication is to be construed as legal advice. R3 does not assume any responsibility for the content, accuracy or completeness of the information presented or for any loss resulting from any action taken or reliance made on any information included in this publication.

About R3

R3 is an enterprise blockchain software firm working with a broad ecosystem of more than 300 participants across multiple industries from both the private and public sectors to develop on Corda, its open-source blockchain platform, and Corda Enterprise, a commercial version of Corda for enterprise usage.

The Corda platform is already being used in industries from financial services to healthcare, shipping, insurance and more. It records, manages and executes institutions' financial agreements in perfect synchrony with their peers, creating a world of frictionless commerce. Learn more at r3.com.