


## COMPLIANCE &amp; RISK

# Compliance considerations for the crypto industry

**Samidh Guha** Founding Partner / Guha PLLC**Sophia Kielar** Associate Attorney / Guha PLLC8 Jan 2024 · 8 minute read 

The federal government's high-profile crackdown on crypto companies requires all crypto market participants to redouble their compliance efforts, both to satisfy regulators and confirm the trust of customers and counterparties

Crypto compliance at this moment demands sophistication. Despite the absence of industry specific statutory or regulatory regimes, several US regulatory and law enforcement agencies have aggressively asserted jurisdiction over the digital asset universe. To date, the U.S.

## Our Privacy Statement & Cookie Policy

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Privacy Statement](#)[Cookie Policy](#)[Cookies Settings](#)[Accept All Cookies](#)

**Comments** by Director of the SEC Division of Enforcement Gurbir Grewal about compliance expectations, particularly concerning individual liability of compliance personnel, should trigger concern for crypto market participants. Grewal emphasized that the SEC would bring actions against compliance personnel “where there was a wholesale failure by compliance personnel to carry out their compliance responsibilities.” This test depends critically on agreement or consensus regarding compliance responsibilities. **With no federal legislation or substantive regulatory framework in place**, unlike with the traditional financial services industry, the possibility increases that even good-faith efforts in crypto are deemed insufficient by regulators and perhaps characterized as “wholesale failures” warranting sanction, per Director Grewal’s public statements.

## Areas of crypto risk

Crypto compliance officers do not have the luxury of waiting for clearer regulations to be promulgated. Instead, they must ensure even amid this uncertainty that their protocols satisfy a host of regulators who have murky and often differing expectations. Certain primary areas of focus, described below, are essential to reduce risk and inspire confidence about a program’s effectiveness.

### *Understanding blockchain technology*

Companies involved in cryptocurrency and their executives must have individuals working on their compliance team who substantively understand blockchain technology, the underpinning of crypto-based activity. Compliance teams must be able to educate employees as to compliance expectations and educate regulators as to their crypto products and operations. Communicating effectively with both constituencies will ensure both a highly functioning and defensible compliance regime.

### *AML procedures*

A core area that compliance strategy must focus on is implementing a satisfactory and robust anti-money laundering (AML) program. Crypto’s decentralized and pseudonymous nature is often viewed suspiciously by regulators as a conduit to hide illicit activity. Indeed, AML experts note that failure to comply with AML requirements is often a part of the **charges that regulatory agencies bring** against companies. Without proper safeguards against money laundering, and the potential for other financial crimes, crypto companies are vulnerable to regulatory scrutiny and exploitation by bad actors.

Crypto asset trading companies must augment traditional AML procedures to include crypto-specific tracking and analysis in their compliance regimens, including using blockchain intelligence tools to identify risky and/or terrorist-associated crypto-wallet addresses. Further, companies should remain conscious of being evaluated under the Bank Secrecy Act (BSA). For example, in October 2022, Bittrex was considered a money services business, ultimately being **fined more than \$24 million** by the Office of Foreign Assets

Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN) — both agencies within the U.S. Treasury Department — for failure to comply with the BSA, AML laws, and other sanctions. Key to the penalties was Bittrex’s access to customer IP and physical address information collected from on-boarding new customers. The company knew numerous customers were located in sanctioned jurisdictions but did not screen customer information for associations with those jurisdictions.

BSA violations by crypto companies could also have criminal consequences. In May 2022, **the former CEO of BitMEX**, one of the oldest and largest convertible virtual currency derivatives exchanges, was sentenced in the Southern District of New York to six months of home detention and a \$10 million fine for violating the BSA by failing to establish, implement, and maintain an anti-money laundering program, including a program to verify the identity of BitMEX’s customers via a properly administered *know your customer* (KYC) program. The company also settled charges with the CFTC and FinCEN in 2021, paying \$100 million for BSA and AML violations.

### ***Retention policies***

Retention policies are a relatively straight-forward proactive step that compliance officers can take to create goodwill with regulators. There are no express regulatory retention requirements for crypto companies, in sharp contrast to express obligations governing the traditional finance space. Nonetheless, regulators deem retention policies as a bellwether of a company’s compliance culture. As but one example, in the recent prosecution and conviction of **FTX founder Sam Bankman Fried**, prosecutors pointed to an absence of a retention policy by FTX as indicia of wrongdoing. Such negative impressions are avoidable. Crypto trading companies should consider creating systems that, as applicable, can log:

- trading data, including profit and loss figures;
- employees trading assets or managing automated trading strategies; and
- the quantity and types of assets traded.

Additionally, crypto-involved companies should consider retention for some years of all company account communications, including not only standard communication methods like email, instant messaging systems, and less traditional communication modes common in the crypto space.

### ***Third-party due diligence***

Crypto-involved companies should be exacting in implementing risk-based approaches when engaging with third-party providers. Regulators have been clear in the traditional finance world that companies are accountable not only for their own compliance obligations, but those of third-party vendors upon which they rely. In fact, the ***Interagency Guidance on Third-Party Relationships: Risk Management*** by the U.S. Federal Reserve, the Federal

Deposit Insurance Corporation (FDIC), and Office of the Comptroller of the Currency, advised that, “[t]he scope and degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship. More comprehensive due diligence is particularly important when a third party supports higher-risk activities, including critical activities.”

This regulatory focus will be magnified in the crypto space. The government views the crypto industry as fundamentally high risk, based often in part on thin understandings of a crypto ecosystem and its novelty. This means that diligence requirements for third parties are very likely to be an expected area of regulatory scrutiny. Marketing and development efforts involving third parties — often leveraging less disciplined mediums like social media, podcasts, and collaborative workshops — create room for misunderstandings and potential problems. Accordingly, as part of a third-party risk assessment program, crypto companies should conduct due diligence on third parties prior to engaging them.

## ***Audits***

Successful and sustainable compliance programs can utilize internal and external audits to get ahead of any issues and demonstrate program’s effectiveness. When done with a regular cadence, audits pressure test compliance programs and provide regulators comfort as to a company’s compliance culture. Given the challenges that many regulators face in understanding the technologies at work and identifying a legal theory of culpability, certain regulators have pointed to weak cultures of compliance with crypto companies as a means for pressing investigations forward.

## ***Privacy and data security concerns***

Operating in a digital environment, the risk of data leaks, cyber-hacks, phishing schemes, and bad actors remains ever present; and because crypto is a booming new industry, scammers have targeted it heavily.

Since crypto uses blockchain technology for verification and does not run through financial institutions, it is also harder to recover the proceeds of theft and its impact. Compliance officers must create tailored provisions that safeguard internal company data, data from partners and consumers, and company and customer assets.

## **Conclusion**

The crypto enforcement landscape continues evolving rapidly but without any sign of greater statutory or regulatory guidance in the immediate future. In December, the **SEC denied a petition by Coinbase** seeking new rules specifically targeting the digital asset sector. The SEC said it would not propose either new rules or long-requested clarification of its expectations because the SEC contends fundamentally that current securities regulations provide crypto companies with sufficient notice of their obligations. This is a premise with



which few, if any, sophisticated crypto professionals agree.

There is no indication that enforcement efforts will slow — if anything, greater enforcement reach is likely, if not certain. Therefore, it is incumbent upon compliance departments and their officers to be proactive in crafting best-in-class compliance programs to continue protecting not only the company and its customers, but also to insulate themselves from enforcement inquiries and potential liability.

---

***Raja Chatterjee contributed to this article. He is a former prosecutor and served as in-house counsel with responsibility for legal, risk, and compliance functions.***

BLOCKCHAIN

COMPLIANCE & RISK

CORPORATES

CRYPTOCURRENCY

DECENTRALIZED FINANCE

DIGITAL TRANSFORMATION & OPERATIONS

FINANCIAL INSTITUTIONS

REGULATORY INTELLIGENCE

RISK MANAGEMENT

US REGULATORS

[← Back to blog](#)

---

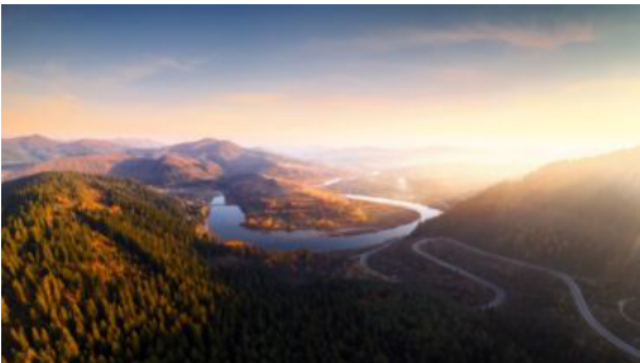
## Solutions



### Thomson Reuters Risk & Fraud Solutions

Now more than ever, organizations need a risk-based, dynamic approach. With risk and fraud solutions from Thomson Reuters, you can tip the balance back towards those doing good in the world. It's time we connected so

Related posts



US companies need to retool their capabilities to reduce child labor violations

24 Feb 2025 · 6 minute read



Fraud-as-a-Service: Creating a new breed of fraudsters

21 Feb 2025 · 7 minute read



Search



ABOUT THOMSON REUTERS

About us  
Annual report  
Careers  
Digital accessibility  
Investor relations  
Press releases  
Site map  
Social impact

PRODUCTS & SERVICES

All products  
Core publishing solutions  
Corporations  
Government  
Legal  
News & media  
Professional services firms  
Tax & accounting

LEARN MORE

API integration  
Artificial intelligence  
Innovation @ Thomson Reuters  
Partnerships  
Supplier portal  
The Trust Principles  
Thomson Reuters Institute

CONTACTS

Contact us  
Global sites directory  
Investors  
Media relations  
Office locations  
Sales & account inquiries

CONNECT WITH US

Facebook  
Instagram  
LinkedIn  
Twitter  
YouTube

Supply chain transparency

Do not sell or share my personal information and limit the use of my sensitive personal information