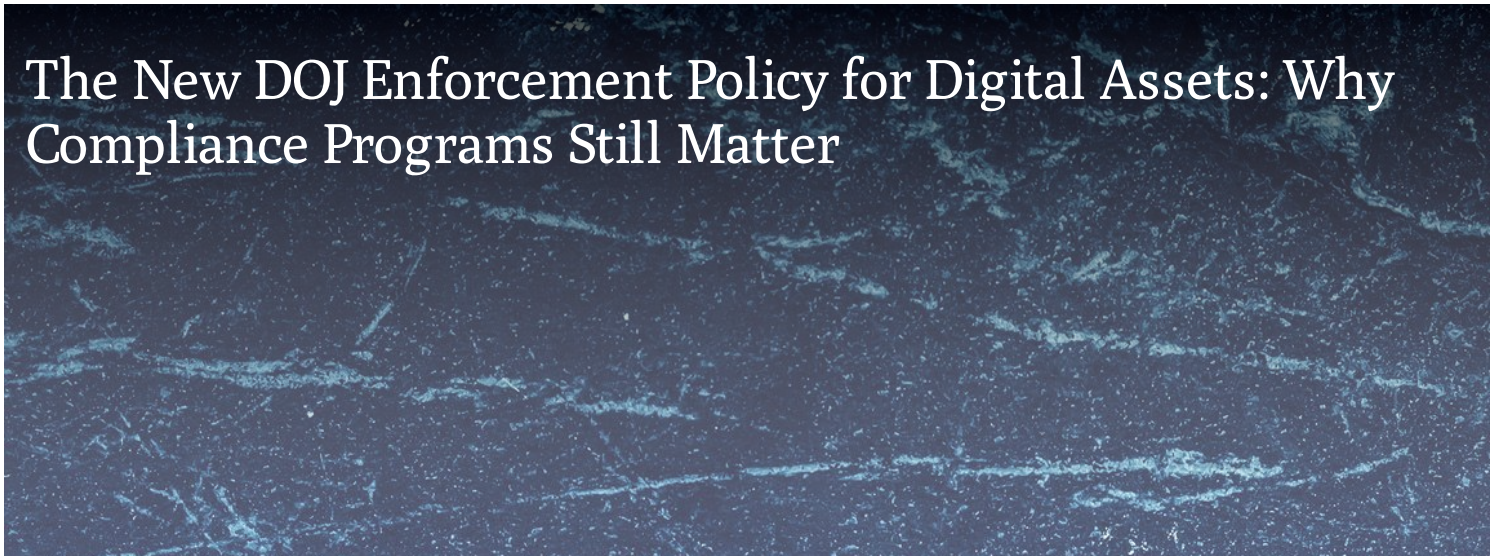
WINSTON & STRAWN LLP

ARTICLE

The New DOJ Enforcement Policy for Digital Assets: Why Compliance Programs Still Matter



MAY 13, 2025

This article was originally published in New York Law Journal. Any opinions in this article are not those of Winston & Strawn or its clients. The opinions in this article are the authors' opinions only.

The Trump administration has continued to implement deep and widespread changes to the Department of Justice (DOJ), including by recently "narrowing [its] enforcement policy relating to digital assets." Dep't of Justice, *Ending Regulation By Prosecution Memorandum* 1 (Apr. 7, 2025).

Among other developments, in furtherance of Executive Orders 14178 and 14157, Deputy Attorney General Todd Blanche issued a memorandum on April 7, 2025 (the April 7 Memo) that instructs federal prosecutors to (1) "no longer pursue litigation or enforcement actions that have the effect of superimposing regulatory frameworks on digital assets," and to instead (2) prosecute individuals who "cause financial harm to digital asset investors and consumers" and "use digital assets in furtherance of other criminal conduct, such as fentanyl trafficking, terrorism, cartels, organized crime, and human trafficking and smuggling."

Pursuant to this shift, prosecutors will "as a matter of discretion" refrain from charging "regulatory violations in cases involving digital assets," including, but not limited to, the following:

- Unlicensed money transmissions under 18 U.S.C. §1960(b)(l)(A) and (B);
- Violations of the Bank Secrecy Act ("BSA");
- Violations relating to unregistered securities;
- Violations relating to unregistered broker-dealers; and
- Other violations of registration requirements under the Commodity Exchange Act.

Notably, the April 7 Memo contemplates a carve-out whereby the foregoing *may* be prosecuted where "there is evidence that the defendant knew of the licensing or registration requirement at issue and violated such a requirement willfully."

The April 7 Memo further directs prosecutors to refrain from charging violations of the Securities Act of 1933, the Securities Exchange Act of 1934, and the Commodity Exchange Act—or the regulations promulgated pursuant to

these Acts—where:

- The charge would require the DOJ to litigate whether a digital asset is a "security" or a "commodity," and
- There is an adequate alternative criminal charge available, such as mail or wire fraud.

Exceptions to this policy are required to be approved by the Deputy Attorney General or his designee(s).

Finally, the April 7 Memo instructs prosecutors to close ongoing investigations "that are inconsistent with the foregoing," disbands the National Cryptocurrency Enforcement Team, a branch of the DOJ's Criminal Division that had been established to identify, investigate, support, and pursue cases involving the criminal use of digital assets, and it directs the Criminal Division's Market Integrity and Major Frauds Unit to "cease cryptocurrency enforcement in order to focus on other priorities, such as immigration and procurement frauds."

While these changes signal a more lenient digital asset enforcement environment, companies must maintain robust cryptocurrency compliance programs for at least the three reasons discussed below.

1. The Law Has Not Changed

Notwithstanding the DOJ's shifts in policy and resource allocation, the underlying laws regulating digital assets remain firmly in place. For example, BSA/anti-money laundering (AML) laws and regulations continue to carry significant penalties and could be enforced by a subsequent administration, through the duration of the statute-of-limitations period. *See* 31

U.S.C. §5321(b) (providing a six-year statute of limitations for civil violations of the BSA); 18 U.S.C. §3282(a) (providing a five-year statute of limitations for criminal violations of the BSA). Indeed, the April 7 Memo itself expressly warns:

This guidance is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

Moreover, the April 7 Memo notes circumstances in which digital currency companies may still be prosecuted for certain crimes. The DOJ will still prosecute actions deemed to be "in furtherance of criminal offenses such as terrorism, narcotics and human trafficking, organized crime, hacking, and cartel and gang financing by cartels."

It will also continue prosecuting regulatory violations where a company has "willfully" flouted a regulatory requirement. And, violations of the Securities Act of 1933 and the Commodity Exchange Act may still be charged where no adequate alternative criminal charge is available, or where the Deputy Attorney General or designee approves of an exception.

Finally, a future DOJ, or even the current one, could at any time decide to reinstate rigorous enforcement of any or all applicable federal laws. By ensuring that their compliance programs are robust and up to date, digital asset companies will be better prepared for such possibilities.

Such programs will help ensure, too, that companies are not held liable under any of the stated carve-outs contemplated by the April 7 Memo (e.g., for "willfully" violating any federal requirement).

2. State and Foreign Regulators Will Continue—and Perhaps Even Increase—Their Enforcement Efforts in the Digital Assets Space

Many states have their own securities laws and anti-fraud statutes that provide independent bases for enforcement. *See* Rich Weber, Seth Farber, & Samantha Osaki, *What Now for White Collar? As the DOJ Steps Back, Will Others Step Up?*, N.Y.L.J. (Mar. 17, 2025).

For example, state and local enforcers in New York, including New York's Department of Financial Services (DFS), the New York Attorney General's Office, and the New York County District Attorney's Office, have already been enforcers in the digital assets industry.

DFS has signaled its intent to fill the gaps in the wake of the DOJ's new enforcement policies, focusing on consumer protection and ensuring financial services companies' compliance.

For instance, DFS Superintendent Adrienne Harris has emphasized that DFS would "keep running [its] drill" on cryptocurrency enforcement, and that it intends to remain at the forefront of regulating AI, cryptocurrency, and cybersecurity. Oscar Gonzalez, *DOJ disbands crypto investigation unit, another sign of the Trump administration's support of digital currency*, ComplianceWeek (Apr. 8, 2025).

Indeed, on April 10, DFS issued a consent order to Block, Inc., a digital asset company that owns a substantial amount of cryptocurrency, with a civil monetary penalty of $40,000,000 and institution of an independent monitorship, for failing to maintain an effective and compliant AML program, among other deficiencies.

Similarly, the New York Attorney General's and New York District Attorney's Offices have broad authority to bring civil and criminal enforcement actions under New York's expansive Martin Act.

Indeed, a recent decision in an enforcement action brought by the NYAG against Gemini Trust Company and Genesis Global Capital rejected those defendants' arguments that their digital assets were not securities under New York law and upheld the application of the Martin Act on that basis. *See* Aislinn Keely, *Crypto Firm DCG Can't Dodge NY AG Suit Over Genesis Woes*, Law360 (Apr. 14, 2025).

And, of course, New York is not alone. Regulators in other states who also disagree with the Trump administration's law enforcement philosophies will likely be similarly aggressive.

For example, in a somewhat parallel situation, California Attorney General Rob Bonta recently issued an "Alert to Businesses" warning them that, although the Department of Justice had paused enforcement of the Foreign Corrupt Practices Act, "the FCPA remains binding federal law and violations are actionable under California's Unfair Competition Law." Press Release, Cal. Dep't of Justice, Office of the Att'y Gen., *Legal Advisory: Alert to Business on Violations of the Foreign Corrupt Practices Act* (Apr. 2, 2025).

It would be no surprise if Attorney General Bonta were to adopt such a stance with respect to enforcement in the digital asset industry in the wake of the DOJ's similar retreat in this area.

Multinational corporations will also remain exposed to foreign agencies that could, in turn, fill in enforcement gaps left by the DOJ. For instance, the United Kingdom's National Crime Agency is increasingly treating digital asset businesses as major players in the fight against serious and organized crime. *See* Jason G. Allen et al., *Legal and Regulatory Considerations for Digital Assets* 34–37.

In the European Union, the Markets in Crypto Assets Regulation ("MiCA") regulates public offers of crypto-assets. *See* ESMA, Markets in Crypto-Assets Regulation, https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica.

MiCA empowers regulators to impose substantial fines on individuals and entities found to violate its provisions, with penalties ranging from "EUR 5,000,000 in flat sums or from 3% up to 12.5% of the total annual turnover, depending on the scope of the infringement." InnReg, Markets in Crypto-Assets Regulation (MiCA) Updated Guide (2025), https://www.innreg.com/blog/mica-regulation-guide.

3. Weak "Know Your Customer" (KYC)/AML Controls Create a Field Day for Bad Actors

While the April 7 Memo may suggest that the DOJ won't pursue companies that unknowingly allow bad actors to launder funds through their platforms, turning a blind eye to BSA, KYC, and AML obligations—especially when red flags are ignored—effectively opens the door for abuse. Weak KYC is a weak link.

Fraudsters seek out platforms with lax compliance protocols to move stolen funds quickly and anonymously, and that illegal activity creates a substantial risk for those platforms of regulatory enforcement both today and in the future.

Digital assets continue to serve as vehicles for financing and facilitating a wide spectrum of high-priority criminal conduct, including fentanyl trafficking, terrorism, transnational cartel operations, organized crime, and human trafficking and smuggling.

These are precisely the types of crimes that the April 7 Memo emphasizes as priorities for the current administration. Failure to maintain adequate BSA, KYC, and AML controls also leaves companies vulnerable to private lawsuits, alleging that they failed to prevent illicit activities, which can damage both their reputation and investor trust. *See, e.g.*, Kateryna Perera, *Block Execs Failed To Prevent 'Illicit Activities,' Suit Says*, Law360 (Apr. 18, 2025).

Further, turning a blind eye to these obligations today could also lead to more aggressive DOJ scrutiny in the future should enforcement priorities shift.

Beyond legal risk, enabling the movement of criminal proceeds, even unintentionally, erodes user trust and undermines the integrity of a business. Companies who operate without robust BSA, KYC, and AML controls lack the ability to assess the origins and purposes of the funds moving through their platforms.

Without those controls, companies may not even be aware of the nature of the criminal enterprises they are enabling—let alone able to halt or report such activity.

Moreover, ongoing and visible compliance efforts in these areas are essential to fostering and maintaining a culture of compliance within an organization. Businesses that begin to selectively deprioritize BSA, KYC, or AML responsibilities send a signal to their employees that compliance is merely a legal checkbox, not a reflection of the organization's core values.

Such a message can create an atmosphere in which other regulatory obligations are viewed as optional or negotiable.

For these reasons, enforcement and compliance surrounding KYC/AML standards are not only about legal adherence—they are central to the integrity of the businesses that implement those controls.

Key Takeaways

While the DOJ's shift in priorities may reduce or narrow certain federal enforcement actions, companies must continue their cryptocurrency compliance programs. Regardless of whether prosecutors choose to enforce relevant federal laws today, the DOJ very well may do so again.

Moreover, recent examples such as DFS's action against Block, Inc., serve as powerful reminders that state and local enforcers may line up to fill in any gaps in enforcement left by the DOJ. Finally, robust compliance programs remain essential to mitigating legal and reputational risks in this evolving regulatory landscape.

8 Min Read

Related Topics

Department of Justice (DOJ) | DOJ Investigations | White Collar

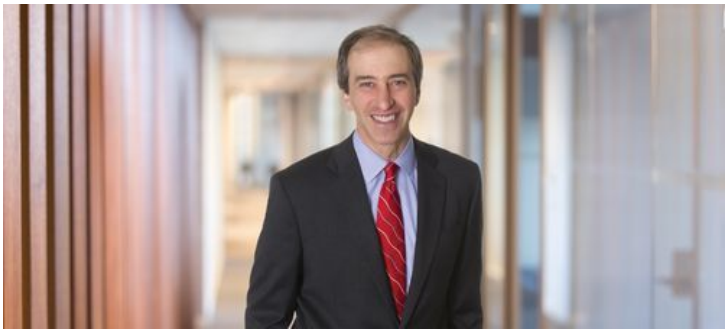
Related Capabilities

Government Investigations, Enforcement & Compliance

Cryptocurrencies, Digital Assets & Blockchain Technology

Related Professionals

Richard Weber



Seth Farber

Samantha Osaki

Annette Lynn Favetta