View on our website.

GIBSON DUNN

Fintech & Digital Assets | Crypto Resource Center Update

August 5, 2025

Update on the U.S. Digital Assets Regulatory Framework – Countering Illicit Finance

This update provides a sequential discussion of the President's Working Group on Digital Asset Markets' description of the intersection of digital assets and illicit finance in its Report.

Government officials have stated that they aim to establish a clear regulatory framework for digital assets, while encouraging innovation and enabling a pathway of compliance for eligible current market participants. Given the Administration's stated agenda is to transform the United States into a global leader in digital assets and blockchain technology, and Congressional support for this agenda, there is a good chance that there will be a set digital asset regulatory framework, with rulemakings and specific guidance to follow.

On July 30, 2025, the President's Working Group on Digital Asset Markets (PWG) published the Strengthening American Leadership in Digital Financial Technology Report (Report) in response to Executive Order 14178. The Report reiterates the Administration's support for digital assets and provides a roadmap of recommendations for Congress and regulators to update the U.S. digital asset regulatory framework, including in connection with digital asset market structure, banking and payments, countering illicit finance, and taxation. The Report emphasizes the need for a clear, fit-for-purpose system to foster innovation, protect investors, and position the United States as a global leader in digital financial technology.

Below is a sequential discussion of the PWG's description of the intersection of digital assets and illicit finance in the Report. The PWG provides an overview of its view of the extent and types of risks in the digital asset space and outlines recommendations for the U.S. government's strategic responses. The Report emphasizes the need for updated regulatory frameworks, stronger but more targeted enforcement, strong cybersecurity practices to prevent attacks, and enhanced cooperation to mitigate systemic vulnerabilities. For additional information on the Report's recommendations for market structure, banking, payments, and taxation, please see our accompanying Client Alert. In addition, for a fulsome discussion on the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), see our prior publication.

I. Illicit Finance Risks

The Working Group begins by noting that the technology underlying digital assets enables ways to mitigate the risk of illicit transactions, and noting that the share of illicit finance transactions conducted using digital assets remains quite small, citing estimates placing illicit transactions at between 0.61% and 0.86% of all on-chain digital asset volumes. Still, the Working Group caveats that the harm from such illicit activity may not be commensurate with the comparatively low transactional value and lists funding of DPRK's miliary efforts and losses from investment schemes as examples of activity that cause more harm than the dollar value might otherwise suggest.

The Report suggests that illicit actors may be attracted to the digital asset ecosystem primarily due to digital asset service providers with weak or nonexistent controls for anti-money laundering (AML) and combatting the financing of terrorism (CFT) risks, as well as the availability of tools and methods such as mixers, anonymity-enhanced cryptocurrencies (AECs), and chain hopping that can hinder law enforcement investigations. Finally, the Report posits that illicit actors also seek to exploit pseudonymity of self-custody and peer-to-peer payments in DeFi networks to conceal or quickly move illicit proceeds.

Key Considerations and Questions

- Will the Administration and Congress use the Report's illicit finance conclusions to guide regulation and legislation moving forward?
- What steps should traditional financial institutions that interact with the digital asset ecosystem take in light of the Report's conclusions?

II. Improving the AML/CFT and Sanctions Frameworks

The PWG next explains that mitigating and combatting the risks posed by illicit use are paramount to protecting the digital asset ecosystem and its users, and ultimately will serve to encourage further innovation and responsible use of digital assets. To carry out that goal, the PWG advocates for clear obligations that are tailored to the risk and structure of the digital asset industry while simultaneously respecting lawful use of digital assets and respecting Americans' privacy rights. This section of the Report also promotes more supportive infrastructure to help digital asset businesses meet AML/CFT requirements. For example, many actors, particularly in the DeFi space, lack clarity on their obligations or the tools to implement effective compliance

programs. The Report recommends targeted guidance for high-risk market segments and better coordination among U.S. regulators to reduce uncertainty.

The PWG makes some regulatory and legislative suggestions that could dramatically reshape how AML and CFT applies to both institutions and individuals within the digital asset ecosystem. First, the PWG suggests that Treasury revisit FinCEN's 2013 and 2019 guidance documents related to the digital asset sector, which have stood as some of the preeminent guidance as to AML/CFT as applied to digital assets for years. Second, the PWG proposes that Congress amend the Bank Secrecy Act to provide further gradations in terms of how certain AML obligations apply to different financial institutions, with obligations based on the type of financial entity (e.g. "financial institution types or sub-types") and also potentially by activity (e.g. "utiliz[ing] smart contracts"). The PWG also proposes legislative amendments to clarify the BSA's extraterritorial reach, which could have important effects on the obligations of foreign-located actors. At the same time, the Working Group also recommends that Congress codify principles reinforcing the ability of individuals to lawfully hold or custody their own digital assets and engage in lawful, direct digital asset transfers without any financial intermediary.

Key Considerations and Questions

- Industry specific guidance has led to more cooperation within certain industries, like casinos or banking. Digital asset providers should consider how gradated obligations might affect their relationships within their market category.
- Some of the Working Group's suggestions could mean that far more foreign-located actors are covered by the BSA. Market participants should review any forthcoming guidance carefully.

III. Equipping Digital Asset Actors to Mitigate Risk

Beyond fortifying AML/CFT frameworks, the PWG advocates for ways to increase the partnership between the public and private sectors. This section proposes expanding private sector authority to investigate and share information pertaining to illicit finance through safe harbors, and touts the benefits of prior efforts within Treasury to learn through round tables that convene an array of private sector and law enforcement professionals. While cautioning against the potential to infringe on civil liberties, the PWG nonetheless advocates for greater information sharing among a broader set of institutions to foster a safer digital asset ecosystem.

Key Considerations and Questions

If implemented, these suggestions could have a major impact on private sector tracing and blockchain analytics firms.

IV. Disrupting and Mitigating Systemic Illicit Finance Risks

The final section calls for proactive measures to dismantle networks that enable systemic illicit finance. The PWG advocates that Treasury should have expanded authority to restrict fund transmission and for continued use of OFAC sanctions in instances in which digital assets are used for specific illicit risks, like crimes targeting Americans, laundering proceeds or illicit drug

and narcotics sales, and financing terrorist organizations. The section also proposes amendments that could expand law enforcement authority related to digital assets, from forfeiture laws to bank fraud statutes. In addition to highlighting some of the ways that Treasury is already working to reduce the risk of malicious cyber actors and advocating for greater public-private partnerships and information sharing, the PWG also recommends that relevant agencies develop principles-based requirements and standards for digital asset firms to address the risks of various industry participants and activities, such as those involving custody and smart contracts.

Key Considerations and Questions

- Some of the PWG's suggestions may have less impact, given how law enforcement already uses available authorities.
- Other proposed changes could potentially lead to far more law enforcement action. For example, the Working Group proposes amending 18 U.S.C. § 1014 to cover *all* false statements in connection with obtaining or maintaining access to financial institution services, rather than solely false statements in loan and credit applications, and to include digital asset service companies within the definition of "financial institution." Such a change could lead to further investigations and enforcement actions, even when the exchange or bank is not itself at risk of losing its funds.
- If implemented, the PWG's recommendation to develop principles-based requirements and standards could mean that digital asset market participants—custodians, wallet providers, etc.—are required to have security tools in place to prevent bad actors from engaging in attacks that lead to illicit finance on the blockchain.

V. PWG Recommendations

To implement the Trump Administration's policy of encouraging innovation and responsible use of digital assets, the PWG states that the United States must protect the digital asset ecosystem and its users by implementing tools and measures to prevent attacks that lead to illicit finance activities and mitigating and combating the risks posed by illicit use. In light of the PWG's emphasis on protecting market participants, proactively preventing the initial attack may be considered priority, given that blockchain transactions are immutable and thus cannot be reversed (as in some traditional financial sectors) after illicit finance activity is identified. The PWG proposes several measures towards this goal of deterring and combating illicit finance. These recommendations take a "whole of government" approach to disrupting and exposing illicit activity in the digital asset ecosystem, while also building confidence among U.S. users and firms seeking to grow domestically. Overall, the recommendations also build on themes that the Administration has articulated in other regulatory contexts as well:

- Specificity: clear frameworks that expressly identify or define which types of actors or entities are subject to various laws and regulations (*e.g.*, defining financial institutions and DeFi networks).
- Tailoring: regulations are no more restrictive than necessary to curtail identified risks (*e.g.*, AML/CFT regulations by entity type).
- Balancing: appropriately consider individual privacy rights and burden to industry when regulating to mitigate risk (*e.g.*, CVC mixing rule, SARs).

The recommendations are largely bifurcated between Treasury and Congress, representing a dual-tracked and whole-of-government approach to fortifying the digital asset ecosystem.

Digital Assets Policy Recommendations		
Topic	**Congress**	**Treasury**
Financial Institutions	Statutory changes to define which entities are subject to the BSA, particularly as Congress considers changes to market structure and the creation of new types of financial institutions. Expand BSA applicability to foreign-located actors based on conduct and effects.	Tailor AML/CFT obligations by entity type. Adopt rules required under the GENIUS Act to treat permitted payment stablecoin issuers as financial institutions. Tailor AML/CFT obligations for payment stablecoin issuers. FinCEN should reconsider its 2013 and 2019 guidance given legislative and regulatory change.
DeFi	Define various actors in DeFi ecosystem and clarify which obligations apply to entities with some, but not all, DeFi characteristics. Codify principles affirming the right to self-custody. Codify that software provides that do not maintain total independent control over value are not engaged in money transmitters.	Tailor obligations to DeFi actors based on their role and associated risks. Reconsider proposed rule on CVC mixing in light of illicit finance risk, privacy and burden to financial sector.
Supervision	--	Provide needed guidance (alongside Federal banking agencies) clarifying AML/CFT obligations and expectations for financial institutions offering digital asset services.
BSA Reporting	Ensure BSA-required reporting to FinCEN under 31 U.S.C. 5331 aligns with IRS reporting rules to coordinate treatment of fiat and digital asset transactions.	Evaluate modernizing Suspicious Activity Report (SAR) reporting, including SAR form updates for digital asset-specific data.
Sanctions	--	Solicit sanctions compliance feedback from DeFi developers and technologists. Update OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry.
Privacy	--	Coordinate with the National Institute for Standards and Technology and other agencies to identify new approaches to

		customer identification in digital asset use cases. Gather information on tools for detecting illicit activity, including digital identity verification. Issuing guidance to financial institutions on using digital identity solutions in customer identification programs.
Investigations	Enact a digital asset-specific "hold law" to provide safe harbor for voluntary asset holds while institutions investigate risk of illicit activity.	Encourage greater information sharing between the public and private sectors via FinCEN's 314(a) and 314(b) programs.
Treasury Authorities	Add a sixth special measure to Section 311 allowing FinCEN to restrict certain digital asset transfers.	Continue using OFAC's sanctions authorities to combat illicit digital asset use.
Law Enforcement	Streamline victim compensation regulations and improve asset-forfeiture efforts in the digital assets space. Amend bank fraud statutes and associated sentencing guidelines to apply to institutions offering digital assets. Amend the National Stolen Property Act, anti-tip-off provisions and forfeiture laws to apply equally to digital assets.	--
Cybersecurity	--	Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) should identify opportunities to increase information sharing, including by providing U.S. regulated digital asset firms access to the Automated Threat Information Feed. OCCIP should harness existing public-private partnerships to identify gaps in addressing operational resiliency. Develop principles-based requirements and standards, as appropriate, for digital asset firms (along with other relevant agencies).

The following Gibson Dunn lawyers prepared this update: M. Kendall Day, Stephanie Brooker, Ro Spaziani, Jeffrey Steiner, Ella Alves Capone, Sam Raymond, Rachel Jackson, and Karin Thrasher.

Gibson Dunn's lawyers are available to assist with any questions you may have regarding these developments. To learn more, please contact the Gibson Dunn lawyer with whom you usually work, any leader or member of the firm's Fintech & Digital Assets practice group, or the authors:

M. Kendall Day – Washington, D.C. (+1 202.955.8220, kday@gibsondunn.com)

Stephanie Brooker – Washington, D.C. (+1 202.887.3502, sbrooker@gibsondunn.com)

Ro Spaziani – New York (+1 212.351.6255, rspaziani@gibsondunn.com)

Jeffrey L. Steiner – Washington, D.C. (+1 202.887.3632, jsteiner@gibsondunn.com)

Ella Alves Capone – Washington, D.C. (+1 202.887.3511, ecapone@gibsondunn.com)

Sam Raymond – New York (+1 212.351.2499, sraymond@gibsondunn.com)

Rachel Jackson – New York (212.351.6260, rjackson@gibsondunn.com)

Karin Thrasher – Washington, D.C. (202.887.3712, kthrasher@gibsondunn.com)