

GIBSON DUNN



Anti-Money Laundering Update

January 9, 2026

2025 Year-End Developments in Anti-Money Laundering

To our clients and friends, this alert is the latest installment of our semi-annual digest in which we review major trends and developments in anti-money laundering (AML) regulation and enforcement during the preceding six months..

Anti-money laundering enforcement clearly remains a high priority for the second Trump Administration, particularly related to key areas of focus like national security and transnational criminal organizations (TCO). In the last few months, the Trump Administration has brought sweeping enforcement actions, and undertaken numerous regulatory developments. These have made clear that financial institutions must maintain rigorous compliance programs to ensure that they conform with the Bank Secrecy Act, particularly to avoid interactions with TCOs and to mitigate risks around national security.

Below we discuss major Trump Administration priorities and guidance as well as notable new federal enforcement actions, significant updates to earlier cases, and key legislative and regulatory developments. We also overview important enforcement actions taken by states and self-regulatory organizations. We conclude with some thoughts about how the Trump Administration priorities will continue to impact AML law, policy, and enforcement going forward.

1. Trump Administration Guidance

As we noted in the [Mid-Year update](#), key players in the Trump Administration issued a range of orders and guidance setting forth enforcement priorities in the months after President Trump was

inaugurated. President Trump first signed an Executive Order aimed at combatting “overcriminalization in federal regulations.”^[1]

1. Department of Justice Statements Regarding Enforcement

The Department of Justice played a critical role in carrying forward the Administration’s vision for AML enforcement, particularly in guidance announcements related to digital assets and other novel technologies. In April 2025, Deputy Attorney General Todd Blanche issued a memorandum entitled “Ending Regulation by Prosecution” focused on the digital assets space. In his memo, Deputy Attorney General Blanche stated that “[t]he Justice Department will no longer pursue litigation or enforcement actions that have the effect of superimposing regulatory frameworks on digital assets while President Trump’s actual regulators do this work outside the punitive criminal justice framework.” The memo contrasted disfavored prosecutions premised solely on regulatory violations against cases that DOJ will prioritize, like criminal conduct that “(a) cause financial harm to digital asset investors and consumers; and/or (b) use digital assets in furtherance of other criminal conduct.” The memo did not wholly reject enforcement actions for regulatory violations in the digital assets space; instead, it stated that such action should only be pursued if “there is evidence that the defendant knew of the licensing or registration requirement at issue and violated such a requirement willfully.”

On August 21, 2025, Acting Assistant Attorney General Matthew Galeotti further outlined the Department of Justice’s approach in technology-based cases, noting that “[w]hen bad actors exploit new technologies, it undermines public trust in those technologies and stifles innovation.” Galeotti emphasized that prosecutors “are not regulators” and will not charge regulatory violations as crimes absent evidence of willfulness.^[2] Accordingly, and consistent with the April 2025 Ending Regulation by Prosecution Memorandum, Galeotti reiterated that DOJ will not bring charges for unlicensed money transmission under 18 U.S.C. § 1960(b)(1)(A) or (B), which criminalize money transmission without the requisite state license or FinCEN registration, respectively, unless the violation was done willfully.

These and other statements are also consistent with the Criminal Division’s broader description of its White-Collar Enforcement Plan. That Plan stated the Criminal Division would focus on “conduct that threatens the country’s national security, including threats to the U.S. financial system by gatekeepers,” “complex money laundering” and “willful [registration and compliance violations] that facilitate significant criminal activity.”^[3]

1. **FinCEN’s Efforts to Clarify Regulatory Expectations and Reduce Regulatory Burden**

Consistent with DOJ’s focus on avoiding regulation by prosecution and instead focusing on issuing clear rules, FinCEN has issued guidance documents intended to clarify expectations on regulated parties and to reduce compliance friction.^[4] For instance, on September 5, 2025, and October 9, 2025, FinCEN issued guidance documents addressing two issues related to Suspicious Activity Reports (SARs): confidentiality (Cross-Border Guidance)^[5] and prioritization (Prioritization Guidance).^[6] Consistent with Director Andrea Gacki’s testimony before the House Committee on Financial Services in September 2025,^[7] the guidance documents assert they will

reduce industry compliance burdens and equip financial institutions to more efficiently produce the type of reports that are most useful to law enforcement.

The Cross-Border Guidance emphasizes that voluntary information sharing can provide a “more complete picture of threats, risks and vulnerabilities” to help financial institutions “better detect and prevent illicit finance activity.”^[8] Clarifying that the BSA generally does not prohibit cross-border information sharing of “underlying facts, transactions, and documents” among financial institutions so long as confidentiality is preserved, the Guidance provides an illustrative list of information that may be shared without violating the confidentiality of SARs, including transaction information, customer/account information, investigative or analytic materials.^[9]

In addition, the Prioritization Guidance confirms that transactions near the \$10,000 currency transaction report (CTR) threshold do not automatically require a SAR; institutions must still assess whether activity is designed to evade CTR obligations and involve at least \$5,000 in funds. The Prioritization Guidance further reiterates the suggested timeline for institutions that elect to file continuing activity SARs, clarifies that institutions are not required to conduct separate continuing-activity reviews after filing a SAR, and confirms that institutions are not required to document no-file decisions.^[10]

Both releases further signal a move by FinCEN to reduce compliance burdens and enable institutions to prioritize reporting most valuable to law enforcement, both generally and in light of DOJ’s stated enforcement priorities. Although time will tell how these policy directives are implemented by examiners on the ground, the releases and similar announcements are helpful for financial institutions responding to inquiries regarding the effectiveness of their AML programs.

1. Prudential Regulator Efforts to Tailor and Clarify Regulatory Expectations

Prudential regulators have also taken steps to clarify and tailor regulatory requirements and supervisory expectations for covered institutions. Although regulators have signaled an intention to focus supervisory resources on material financial risks,^[11] they have also emphasized the need to tailor AML-related requirements to institution size, complexity, and risk profile and have issued additional guidance to reduce compliance burdens without undermining core AML objectives.

For example, building on the Office of the Comptroller of the Currency’s (OCC) broader initiative to tailor risk-based supervision and align regulatory and supervisory expectations with the business models of smaller institutions, on November 24, 2025, the OCC issued new guidance revising the agency’s application of the BSA/AML examination procedures for community banks (now defined as institutions with up to \$30 billion in assets).^[12] The OCC explained that community banks generally present lower money-laundering and terrorist-financing risk profiles, and that the revised approach permits examiners to focus on a bank’s actual risk profile rather than prescriptive procedural baselines that may be disproportionate to the risks presented. As part of this recalibration, the OCC also announced that it will no longer collect information from community banks through the Money Laundering Risk (MLR) system, eliminating a longstanding reporting requirement.^[13]

Additionally, on July 31, 2025, federal banking agencies, with the concurrence of FinCEN, clarified that banks and credit unions subject to the Customer Identification Program (CIP) rule may obtain taxpayer identification numbers (TIN) from third parties rather than directly from the customer.^[14] Shortly thereafter, on August 5, 2025, the FDIC issued a supervisory letter explaining that the CIP rule's requirement to collect identifying information "from the customer" does not prohibit the use of pre-filled information. The FDIC clarified that institutions could use information from current or prior accounts or relationships involving the bank or its agents, or other sources, to pre-fill information provided that information is reviewed, corrected, undated and confirmed by the customer.^[15]

Finally, the OCC previewed that it may make additional changes to how it approaches BSA/AML supervision as part of its work to combat debanking, another priority of the Trump Administration.^[16] Pursuant to that work, the OCC issued a bulletin reminding banks of the limited circumstances that allow for the release of customer financial records and the proper use of SARs.^[17] The bulletin states that banks "should not use voluntary SARs as a pretext to improperly disclose customers' financial information or evade the [Right to Financial Privacy Act]. A bank should only submit a voluntary SAR where it identifies concrete suspicious activity, such as activity that could form the basis for filing a SAR except that it is under the applicable threshold."

1. Federal Enforcement Actions

1. Alleged Willful Registration and Compliance Violations that Facilitate Significant Criminal Activity

Consistent with statements referred to above by the Criminal Division and the Deputy Attorney General, recent prosecutions for compliance and registration violations have highlighted offenses that were willful and that facilitated underlying criminal activity.

1. Former President of Oklahoma Bank

In December 2025, the Department of Justice announced the indictment and arrest of the former President and Chief Executive Officer of an Oklahoma bank for failure to implement an adequate AML program in violation of the Bank Secrecy Act, among other charges, in the U.S. District Court for the Western District of Oklahoma.^[18] According to DOJ, the defendant, who also acted as the bank's Chief Financial Officer, Information Technology Officer, Bank Secrecy Act Officer, and Compliance Officer at various points between February 2007 and September 2024, allegedly caused the now-failed bank to issue loans to certain customers that were never repaid, manipulated the bank's records to falsely overstate the performance of the loans, provided false records to both the Office of the Comptroller of the Currency and the bank's Board of Directors, failed to file any suspicious activity reports on his own fraudulent scheme, and advised customers to make cash deposits below \$10,000 to avoid relevant reporting requirements. In other words, the charges in this case exemplify both of the Administration's priorities: the conduct allegedly was willful, because the defendant acted as Compliance Officer and thus knew of his regulatory obligations under the BSA; and it allegedly fostered underlying criminal activity, because the BSA violations helped conceal his fraudulent scheme.

1. Virtual Trading Platform

On December 9, 2025, an online virtual currency trading platform pleaded guilty in the U.S. District Court for the Eastern District of California to charges that included conspiracy to willfully fail to maintain an effective AML program, in violation of the BSA, and conspiracy to operate an unlicensed money transmitting business, in violation of 18 U.S.C. § 1960(b)(1)(C).^[19] The platform and its founders allegedly marketed the platform as not requiring know-your-customer (KYC) information, allowed customers to use the platform without gathering appropriate KYC information, presented fake AML policies to third parties, and failed to file suspicious activity reports where appropriate. According to DOJ, as a result of these alleged failings, the platform was used as a vehicle for money laundering, sanctions violations, and other criminal activity, including fraud, romance scams, extortion schemes, and commercial sex-related offenses. Pursuant to the plea agreement, the platform agreed to pay a criminal penalty of \$4 million.^[20] This amount represents a reduction based on inability to pay from an agreed-upon fine of \$112.5 million, which, in turn, represented a 25% reduction from the bottom of the applicable sentencing guidelines because of the platform's cooperation. In 2024, one of the platform's co-founders, who acted as chief technology officer, pleaded guilty to conspiracy to willfully fail to maintain an effective AML program, and agreed to pay a \$5 million fine over the course of two years, resign and refrain from future management at the platform.^[21]

Also on December 9, 2025, FinCEN announced a \$3.5 million civil penalty against the platform to resolve a parallel civil investigation into the same conduct.^[22] As a part of the resolution, the platform also admitted they failed to register as a money services business, implement and maintain an effective AML program, and file SARs.^[23] According to the Consent Order, FinCEN agreed to credit \$1.75 million of the platform's criminal penalty paid to DOJ against this civil penalty.^[24]

1. Redirected Digital Asset Enforcement

Prosecutorial decisions in previously charged cases against executives at virtual trading platforms Samourai Wallet and Tornado Cash also illustrate DOJ's shift away from failure-to-register charges and toward knowledge-based offenses under Section 1960(b)(1)(C), emphasizing sanctions, illicit-finance, and national security risks in particular as the Department's primary anti-money laundering priorities.

1. Co-founders of Samourai Wallet

In November 2025, the Honorable Denise Cote of the U.S. District Court for the Southern District of New York sentenced the co-founders of Samourai Wallet to four- and five-year terms of imprisonment, respectively, after their July 2025 guilty pleas to charges of conspiracy to operate an unlicensed money transmitting business. According to the U.S. Attorney's Office, Samourai Wallet was a cryptocurrency service that allegedly facilitated non-traceable private crypto transactions.

Samourai Wallet allegedly processed billions of dollars in transactions and was used to obscure the provenance of criminal proceeds, including for sanctions evasion, and the founders,

according to DOJ, continued to operate and profit from the platform despite their awareness that users relied on Samourai's mixing features specifically to evade law enforcement detection.^[25] The original indictment, unsealed in April 2024, alleged conspiracy to violate both 18 U.S.C. § 1960(b)(1)(B), which criminalizes operating without required FinCEN registration, and Section 1960(b)(1)(C), which targets the knowing transmission of criminal proceeds or funds intended to promote unlawful conduct. However, following the April 2025 Ending Regulation by Prosecution Memorandum, which stated that "[p]rosecutors should not charge regulatory violations in cases involving digital assets . . . under 18 U.S.C. § 1960(b)(1)(A) and (B)," DOJ filed a superseding indictment omitting the Section 1960(b)(1)(B) allegation.^[26] In its sentencing submissions, DOJ focused on actions by the co-founders to allegedly "repeatedly solicit[], encourage[], and invite[] criminals to use Samourai to conceal their transfers of criminal proceeds."^[27]

1. Tornado Cash Verdict

In July 2025, Roman Storm proceeded to trial in the Southern District of New York on charges related to his role in creating and maintaining the Tornado Cash protocol, an open-source crypto anonymity protocol that, according to DOJ, was used to anonymize more than one billion dollars in illicit proceeds. The indictment alleged Storm conspired to commit money laundering, to operate an unlicensed money-transmitting business, and to violate U.S. sanctions. Like the charge in the Samourai Wallet case, the unlicensed-transmission charge was initially predicated on both Section 1960(b)(1)(B) and Section 1960(b)(1)(C), but was amended after the April 2025 Ending Regulation by Prosecution Memorandum.

After a four-week trial, the jury returned a mixed verdict on August 6, 2025. As described in the DOJ press release, the jury convicted Storm of conspiracy to operate an unlicensed money-transmitting business.^[28] The jury, however, was unable to reach a verdict on the money-laundering and sanctions-violation charges, resulting in a mistrial. Both of these charges carry higher penalties. Storm faces up to five years in prison on the unlicensed-transmission conviction, and as of this writing, DOJ has not yet publicly indicated whether it will seek retrial on the hung counts.

1. Swift, Coordinated Action Where Priorities Combine

The Trump Administration has also taken coordinated, multiagency enforcement actions utilizing an array of tools, particularly where its policy priorities—such as national security, TCOs, complex money laundering and financial harm—converge.

1. Prince Group: Coordinated Criminal, Civil, and Sanctions Actions

On October 14, 2025, DOJ and OFAC brought coordinated criminal, civil, and administrative actions against the Cambodian-based "Prince Group." According to the government, the Prince Group is allegedly a vast transnational criminal enterprise built around forced labor scam compounds. At those compounds, individuals are forced to perpetrate "pig butchering" cryptocurrency investment fraud schemes against victims around the world.^[29] On October 14, 2025, the U.S. Attorney's Office for the Eastern District of New York and the National Security Division of DOJ also unsealed a criminal indictment against Chen Zhi. As described in the criminal indictment against alleged chairman Chen Zhi, the Prince Group's public facing real

estate, banking, and hospitality operations masked an extensive criminal infrastructure staffed by trafficked workers compelled to run scripted investment scams that generated billions in victim losses.

The indictment alleges that one local network of the Prince Group operating in Brooklyn allegedly laundered more than \$18 million in victim funds through New York shell companies between 2021 and 2022. On October 14, 2025, DOJ also unsealed a civil forfeiture complaint against approximately 127,271 Bitcoin, then valued at approximately \$15 billion, that was previously seized by the U.S. government and was allegedly the proceeds and instrumentalities of the Prince Group's wire fraud and money laundering schemes.[\[30\]](#) The civil forfeiture complaint alleges that the seized cryptocurrency included illicit proceeds that had been intentionally commingled with newly mined cryptocurrency, funds that had been routed through complex wallet layering structures, including by "spraying" and "funneling" large sums of cryptocurrency by repeatedly disaggregating and re-consolidating the funds to obscure the source of funds, and other means of money laundering.[\[31\]](#)

In a parallel action on October 14, 2025, OFAC designated Prince Group as a Transnational Criminal Organization (TCO) and imposed sanctions on 146 targets associated with the enterprise, including Chen Zhi, key executives, and numerous affiliated companies across Prince Group's global corporate network.[\[32\]](#)

1. Huione

In May 2025, FinCEN issued a finding and Notice of Proposed Rulemaking identifying Cambodian-based Huione Group as a foreign financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act.[\[33\]](#) FinCEN found that Huione functioned as a major laundering hub for criminal activity connected to North Korea, and for TCOs operating large-scale pig butchering and other crypto fraud schemes across Southeast Asia. FinCEN alleged that Huione subsidiaries processed at least 4 billion dollars in illicit proceeds between August 2021 and January 2025.

In October 2025, FinCEN issued the final rule severing Huione Group from the U.S. financial system by, among other things, requiring financial institutions to take steps not to process transactions for the correspondent account of a foreign banking institution in the United States if such a transaction involves Huione Group.[\[34\]](#) In parallel, OFAC announced coordinated sanctions designating Huione Group as a TCO and targeting related entities and individuals involved in laundering scam proceeds and facilitating cybercrime.[\[35\]](#) Treasury described Huione as a central financial conduit for Southeast Asia's scam industry, including networks overlapping with or adjacent to Prince Group's operations.

1. OCC Enforcement Action

On October 16, 2025, the OCC announced a formal agreement with a bank to address unsafe or unsound practices stemming from, among other things, BSA/AML risk management and suspicious activity reporting and related violations of law, rule or regulation.[\[36\]](#) Pursuant to the agreement, the bank committed to adopting a number of written policies and procedures, hiring a

qualified BSA Officer and maintaining sufficient staff to support the BSA Officer and the bank's BSA/AML program, and implementing a number of governance changes.

- **State Enforcement Actions**

State enforcement authorities have continued to take action over the last months of 2025. This is consistent with our analysis from the middle of 2025, noting that state regulators may be more aggressive in light of the perceived deregulatory federal environment.[\[37\]](#)

1. **NYDFS Action against New York Financial Institution**

On August 7, 2025, the New York Department of Financial Services (NYDFS) announced a \$48.5 million settlement with a New York financial institution for its alleged failure to conduct sufficient due diligence on a former business partner, and for other AML deficiencies. The financial institution agreed to pay a \$26.5 million penalty and to invest an additional \$22 million to remediate compliance weaknesses pursuant to a NYDFS-approved plan.

NYDFS concluded that the financial institution failed to adequately monitor allegedly illicit activities occurring through its partner, and highlighted its deficient compliance program, inadequate investigation protocols, gaps in its monitoring system, and lack of defined guidelines for responding to law enforcement requests. NYDFS stated that the resolution underscores its commitment to “ensure accountability, in turn protecting consumers and safeguarding the integrity of the financial system.”[\[38\]](#)

1. **California enforcement action against crypto kiosks**

On October 30, 2025, the California Department of Financial Protection and Innovation (DFPI) announced that it had taken action against crypto kiosk operators for allegedly violating California's Digital Financial Assets Law (DFAL).[\[39\]](#) DFPI concluded that, since January 2024, one such crypto kiosk operator overcharged consumers fees and markups above statutory maximums, accepted cash transactions over DFAL's \$1,000 daily legal limit, and did not provide legally required disclosures before transactions and omitted other key information on receipts.[\[40\]](#) That operator was ordered to pay \$675,000, which included \$105,000 in restitution to overcharged consumers.[\[41\]](#)

2025 marked the first year of enforcement actions under DFAL, which was enacted in 2023. DFPI's press release highlighted enforcement actions it had taken against other crypto kiosks throughout the year, including its first DFAL enforcement action, which was a fine against a crypto kiosk operator, and desist and refrain orders against other crypto kiosk operators.[\[42\]](#)

1. **FINRA Enforcement Actions**

The Financial Industry Regulatory Authority (FINRA) has also been active in the latter half of 2025, including for regulatory or technical violations.

- For example, FINRA took action against a Swiss Private Bank for allegedly failing to “establish and implement policies and procedures for its AML compliance program” by failing to properly monitor wire transfers for suspicious activity, validate the coverage of its

AML monitoring tool, and perform certain periodic account reviews or AML-related investigations.[\[43\]](#) The Private Bank agreed to pay a fine totaling \$650,000.[\[44\]](#)

- FINRA took action against an investment banking and wealth management firm for allegedly failing to conduct independent testing of its AML program for 13 years.[\[45\]](#) The Firm agreed to pay a fine of \$30,000.[\[46\]](#)
- FINRA also took action against an investment bank for allegedly using an incorrect monetary threshold to determine when SARs should be filed and, as a result, failing to timely file 42 SARs within a three-year period.[\[47\]](#) The investment bank agreed to pay a fine of \$500,000.[\[48\]](#)

1. Legislative Developments

On July 18, 2025, the President signed the Guiding and Establishing National Innovation for U.S. Stablecoins Act (the GENIUS Act or the Act) into law.[\[49\]](#) The GENIUS Act is perhaps the most significant United States law affecting the digital assets industry to date and reflects the Administration's and Congress' priorities of establishing a comprehensive framework for the United States' approach to digital assets and related activities. For more detailed information about the GENIUS Act, its requirements, and associated studies or rulemakings, please see our separate [client alert](#).

The Act establishes a Federal regulatory framework for the issuance of "payment stablecoins" and makes it unlawful for any person other than a "permitted payment stablecoin issuer" (Permitted Issuer) to issue payment stablecoins in the U.S.[\[50\]](#) It defines payment stablecoins as any digital asset that is, or is designed to be, used as a means of payment or settlement and the issuer of which (i) is obligated to convert, redeem, or repurchase for a fixed amount of monetary value and (ii) represents that such issuer will maintain, or create the reasonable expectation that it will maintain, a stable value tied to a fixed amount of monetary value.[\[51\]](#) Permitted Issuers include subsidiaries of insured depository institutions with federal approval as well as other state and Federally qualified institutions.[\[52\]](#) If a payment stablecoin is not issued by a Permitted Issuer then it cannot be (i) treated as cash or cash equivalent for accounting purposes; (ii) eligible as cash or cash equivalent margin or collateral for broker-dealers, swap dealers, and other CFTC and SEC intermediaries; or (iii) accepted as a settlement asset to facilitate wholesale payments between banking organizations.[\[53\]](#)

The Act also designates Permitted Issuers as financial institutions under the BSA and subject to the BSA's anti-money laundering, customer due diligence, and transaction monitoring requirements.[\[54\]](#) Permitted Issuers also will be required to file SARs with FinCEN and comply with OFAC sanctions requirements.[\[55\]](#) Additionally, within three years of the Act's enactment, FinCEN will issue guidance and rules based on the research and risk assessments completed by Treasury and outlined in public comments, which FinCEN solicited on August 18, 2025 and September 19, 2025.[\[56\]](#) This guidance will address (a) implementation of innovative techniques by regulated financial institutions to detect illicit activity involving digital assets, (b) standards for payment stablecoin issuers to identify and report illicit activity, money laundering, sanctions evasion, and insider trading, (c) standards for payment stablecoin issuers to monitor the blockchain, digital asset mixing, and tumbler services, and (d) risk management standards for financial institutions and decentralized finance protocols.[\[57\]](#)

1. Conclusion

The latter half of 2025 reflects an AML enforcement landscape shaped by the Trump Administration's coordination of federal enforcement authority within DOJ and Treasury, civil regulators' work to streamline and tailor regulatory obligations, and the states continued to pursuit of aggressive enforcement. We anticipate that 2026 will continue to be active, with the Administration continuing to leverage AML enforcement to advance policy priorities, likely including those focused on national security and transnational criminal organizations. We will continue to monitor these developments and report accordingly on steps individuals and entities should take to navigate the ever-evolving BSA/AML regulatory regime.

[1] Executive Order, Fighting Overcriminalization in Federal Regulations (May 9, 2025), <https://www.whitehouse.gov/presidential-actions/2025/05/fighting-overcriminalization-in-federal-regulations/>. For further insight and analysis, please see our client alert. Gibson Dunn: New Executive Order Seeks to Combat "Overcriminalization in Federal Regulations" (May 16, 2025).

[2] Department of Justice, *Acting Assistant Attorney General Matthew R. Galeotti Delivers Remarks at the American Innovation Project Summit in Jackson, Wyoming* (August 21, 2025), <https://www.justice.gov/opa/speech/acting-assistant-attorney-general-matthew-r-galeotti-delivers-remarks-american>.

[3] Memorandum, U.S. Department of Justice, Criminal Division, *Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime* (May 12, 2025), available at <https://www.justice.gov/criminal/media/1400046/dl?inline>.

[4] As noted below, the GENIUS Act, which creates a framework for regulating permitted payment stablecoin issuers (Permitted Issuers), further calls on the Treasury Department to adopt rules, tailored to the size and complexity of Permitted Issuers, to implement application of the BSA and sanctions laws to Permitted Issuers.

[5] FinCEN, Cross-Border Information Sharing by Financial Institutions and SAR Confidentiality, FIN-2025-G001 (Sept. 5, 2025), <https://www.fincen.gov/system/files/2025-09/Crossborderguidance-508C.pdf>.

[6] FinCEN, FinCEN Issues Frequently Asked Questions to Clarify Suspicious Activity Reporting Requirements (Oct. 9, 2025), <https://www.fincen.gov/news/news-releases/fincen-issues-frequently-asked-questions-clarify-suspicious-activity-reporting>.

[7] FinCEN, Statement by Andrea M. Gacki before the House Committee on Financial Services, Subcommittee on National Security, Illicit Finance, and International Financial Institutions (Sept. 9, 2025), <https://www.fincen.gov/news/testimony/statement-fincen-director-andrea-m-gacki-house-committee-financial-services>.

[8] FinCEN, Cross-Border Information Sharing (FIN-2025-G001).

[9] *Id.*

[10] FinCEN, *FinCEN Issues Frequently Asked Questions to Clarify Suspicious Activity Reporting Requirements* (Oct. 9, 2025), <https://www.fincen.gov/news/news-releases/fincen-issues-frequently-asked-questions-clarify-suspicious-activity-reporting>.

[11] See, e.g., Federal Reserve Board of Governors, Statement of Supervisory Operating Principles (Nov. 18, 2025), <https://www.federalreserve.gov/newsevents/pressreleases/bcreg20251118a.htm>; Unsafe or Unsound Practices, Matters Requiring Attention, 90 Fed. Reg. 48835 (proposed Oct. 7, 2025), <https://www.federalregister.gov/documents/2025/10/30/2025-19711/unsafe-or-unsound-practices-matters-requiring-attention>.

[12] Press Release, Office of the Comptroller of the Currency (Nov. 24, 2025), <https://occ.gov/news-issuances/news-releases/2025/nr-occ-2025-110.html>.

[13] Press Release, Office of the Comptroller of the Currency (Nov. 24, 2025), <https://occ.gov/news-issuances/bulletins/2025/bulletin-2025-38.html>.

[14] Press Release, Federal Reserve Board of Governors (July 31, 2025), <https://www.federalreserve.gov/newsevents/pressreleases/bcreg20250731a.htm>.

[15] Press Release, Federal Deposit Insurance Corporation (Aug. 5, 2025), https://www.fdic.gov/news/financial-institution-letters/2025/fdic-supervisory-approach-regarding-use-pre-populated?source=govdelivery&utm_medium=email&utm_source=govdelivery.

[16] For more information, see our prior alert on debanking [here](#).

[17] Protecting Customer Financial Records, OCC Bulletin 2025-23 (Sept. 8, 2025), <https://occ.gov/news-issuances/bulletins/2025/bulletin-2025-23.html>.

[18] Press Release, Department of Justice (Dec. 4, 2025), available at <https://www.justice.gov/opa/pr/former-president-failed-oklahoma-bank-indicted-bank>.

[19] Press Release, Department of Justice (December 10, 2025), <https://www.justice.gov/opa/pr/virtual-asset-trading-platform-pleads-guilty-violating-travel-act-and-other-federal-criminal>.

[20] *Id.*

[21] *United States v. Schaback*, No. 24-cr-0072 (E.D. Cal Jul. 8, 2024), Dkt. No. 14 (Plea Agreement).

[22] Press Release, Financial Crimes Enforcement Network (December 9, 2025), <https://www.fincen.gov/news/news-releases/fincen-assesses-35-million-penalty-against-paxful-facilitating-suspicious>.

[23] *Id.*

[24] *FinCEN Consent Order Imposing Civil Money Penalty, In the Matter of Paxful, Inc. and Paxful USA, Inc.*, FinCEN Docket No. 2025-02, at 24 (Dec. 9, 2025), (consent order) <https://www.fincen.gov/system/files/2025-12/PaxfulConsentOrder.pdf>.

[25] *U.S. v. Rodriguez*, 1:24-Cr-82, Dkt. No. 1 (Indictment) (S.D.N.Y. Feb. 20, 2024); Press Release, Department of Justice (Nov. 19, 2025), <https://www.justice.gov/usao-sdny/pr/founders-samurai-wallet-cryptocurrency-mixing-service-sentenced-five-and-four-years>.

[26] *Id.*, Dkt. No. 109 (Superseding Indictment) (June 25, 2025).

[27] *U.S. v. Rodriguez*, 1:24-Cr-82, Dkt. No. 157 at 2 (Gov't Sentencing Letter) (S.D.N.Y. Oct. 31, 2025).

[28] Press Release, Department of Justice (Aug. 6, 2025), <https://www.justice.gov/usao-sdny/pr/founder-tornado-cash-crypto-mixing-service-convicted-knowingly-transmitting-criminal>.

[29] Press Release, Department of Justice (Oct. 14, 2025), <https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged>; Press Release, Department of the Treasury (Oct. 14, 2025), <https://home.treasury.gov/news/press-releases/sb0278>.

[30] *United States v. Approximately 127,271 Bitcoin ("BTC") Previously Stored at the Virtual Currency Addresses Listed in Attachment A, and All Proceeds Traceable Thereto*, 1:25-cv-05745, Dkt. 1 (E.D.N.Y. Oct. 14, 2025) (Complaint); Press Release, Department of Justice (Oct. 14, 2025), <https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged>.

[31] *United States v. Approximately 127,271 Bitcoin ("BTC") Previously Stored at the Virtual Currency Addresses Listed in Attachment A, and All Proceeds Traceable Thereto*, 1:25-cv-05745, Dkt. 1 (E.D.N.Y. Oct. 14, 2025) (Complaint).

[32] Press Release, U.S. Dep't of the Treasury (Oct. 14, 2025), <https://ofac.treasury.gov/recent-actions/20251014>

[33] Press Release, FinCEN (May 1, 2025), <https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-money-laundering-concern>.

[34] Press Release, FinCEN (Oct. 14, 2025), <https://www.fincen.gov/news/news-releases/fincen-issues-final-rule-severing-huione-group-us-financial-system>.

[35] Press Release, U.S. Dep't of the Treasury (Oct. 14, 2025), <https://home.treasury.gov/news/press-releases/sb0278>.

[36] Press Release, Office of the Comptroller of the Currency (October 16, 2025), [https://www.occ.gov/news-issuances/news-releases/2025/nr-occ-2025-102.html](https://www OCC.gov/news-issuances/news-releases/2025/nr-occ-2025-102.html).

[37] Mid-Year Developments in Anti-Money Laundering in 2025 (Aug. 4, 2025), <https://www.gibsondunn.com/mid-year-developments-in-anti-money-laundering-in-2025/>.

[38] Press Release, N.Y. State Dep't of Fin. Servs (August 7, 2025), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20250806.

[39] Press Release, Dep't of Financial Protection and Innovation (October 30, 2025), https://dfpi.ca.gov/press_release/dfpi-cracks-down-on-cash-to-crypto-kiosk-operators/.

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] Letter of Acceptance, Waiver, and Consent No. 2021069508201, Financial Industry Regulatory Authority (October 9, 2025), [Click Here](#).

[44] *Id.*, at 1.

[45] Letter of Acceptance, Waiver, and Consent No. 2023077033101, Financial Industry Regulatory Authority (September 8, 2025), [Click Here](#).

[46] *Id.*

[47] Letter of Acceptance, Waiver, and Consent No. 2023079913301, Financial Industry Regulatory Authority (August 22, 2025), [Click Here](#).

[48] *Id.* at 1.

[49] Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), Pub. L. 119-27.

[50] *Id.* at § 3(a).

[51] *Id.* at § 2(22).

[52] *Id.* at § 2(23).

[53] *Id.* at § 3(g).

[54] *Id.* at § 4(a)(5)(A).

[55] *Id.* at § 4(a)(5)(A)(iii), (vi).

[56] *Id.* at § 9(a). See also Press Release, FinCEN (Aug. 18, 2025), <https://home.treasury.gov/news/press-releases/sb0254>; Press Release, FinCEN (Sept. 19, 2025), <https://www.fincen.gov/news/news-releases/treasury-seeks-public-comment-implementation-genius-act>.

[57] *Id.* at § 9(d).

Please click on the link below to view the complete update and endnotes on Gibson Dunn's website:

Read More

The following Gibson Dunn lawyers assisted in preparing this update: Stephanie Brooker, M. Kendall Day, Ella Alves Capone, Sam Raymond, and Rachel Jackson.

Gibson Dunn has deep experience with issues relating to the Bank Secrecy Act, other AML and sanctions laws and regulations, and the defense of financial institutions more broadly. For assistance navigating white collar or regulatory enforcement issues involving financial institutions, please contact any of the authors, the Gibson Dunn lawyer with whom you usually work, or any of the leaders and members of the firm's Anti-Money Laundering / Financial Institutions, Financial Regulatory, White Collar Defense & Investigations, or International Trade practice groups:

Anti-Money Laundering / Financial Institutions:

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

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

White Collar Defense and Investigations:

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

Winston Y. Chan – San Francisco (+1 415.393.8362, wchan@gibsondunn.com)

Nicola T. Hanna – Los Angeles (+1 213.229.7269, nhanna@gibsondunn.com)

F. Joseph Warin – Washington, D.C. (+1 202.887.3609, fwarin@gibsondunn.com)

Global Fintech and Digital Assets:

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

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

Sara K. Weed – Washington, D.C. (+1 202.955.8507, sweed@gibsondunn.com)

Global Financial Regulatory:

William R. Hallatt – Hong Kong (+852 2214 3836, whallatt@gibsondunn.com)

Michelle M. Kirschner – London (+44 20 7071 4212, mkirschner@gibsondunn.com)

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

International Trade:

Ronald Kirk – Dallas (+1 214.698.3295, rkirk@gibsondunn.com)

Adam M. Smith – Washington, D.C. (+1 202.887.3547, asmith@gibsondunn.com)

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

If you would prefer NOT to receive future emailings such as this from the firm,
please reply to this email with "Unsubscribe" in the subject line.

If you would prefer to be removed from ALL of our email lists,
please reply to this email with "Unsubscribe All" in the subject line. Thank you.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit our [website](#).