LOOKING BACK AND MOVING FORWARD: TOP ISSUES SHAPING WHITE COLLAR LAW IN 2026

ATTORNEY ADVERTISING

Ballard Spahr LLP

TABLE OF CONTENTS

1 Tariffs and Customs Enforcement

3 Health Care and False Claims Act

4 Whistleblower Programs

6 Anti-Money Laundering and Countering the Financing of Terrorism, Digital Assets, and Artificial Intelligence

10 Conclusion

LOOKING BACK AND MOVING FORWARD: TOP ISSUES SHAPING WHITE COLLAR LAW IN 2026

As we look back on 2025, it is clear that the landscape of white collar defense and internal investigations continues to evolve amidst an array of complex legal and regulatory challenges. In 2025, businesses faced heightened scrutiny in areas such as tariffs and customs enforcement, while False Claims Act (FCA) cases, particularly those impacting health care, surged. Whistleblower programs have become increasingly active, spurring internal reviews and external enforcement actions. Meanwhile, ongoing concerns about money laundering, cartel activity, cryptocurrency regulation, and the rapid advancement of artificial intelligence are reshaping compliance priorities for organizations across industries. In this report, we review key developments from the past year in these areas and explore what companies can expect in 2026 as enforcement trends intensify and new risks emerge.

TARIFFS AND CUSTOMS ENFORCEMENT

By Henry E. Hockeimer, Jr., Marjorie J. Peerce, and Wilson Smerconish

Prosecutions for the evasion of tariff duties and misrepresentations made on customs forms accompanying imports into the United States have been relatively rare over the years. But with the current Administration's focus on tariffs and ensuring the truth of attestations concerning the nature of the goods imported, the value of those goods, and countries of origin, we expect to see a significant uptick in government enforcement.

Internal organizational shifts and other actions reflect executive agency efforts to turn words into enforcement action. For example, this summer, the Criminal Division of the Department of Justice (DOJ) announced that the Major Frauds Section would substantially focus on tariff enforcement and add attorneys from the previously existing Consumer Protection Branch within the Civil Division. The acting head of the Criminal Division explained that this larger section, "which will be renamed the Market, Government, Consumer Fraud Unit, will focus on trade fraud and other white collar crimes affecting investors and consumers."

Six weeks later, the Administration announced the creation of a new Department of Justice and Department of Homeland Security "Trade Fraud Task Force to bring robust enforcement against importers and other parties who seek to defraud the United States."

Process and Regulatory Framework

When goods are imported into the United States, certain regulatory requirements are triggered. The process begins when the importer purchases foreign goods, and the seller ships them to a U.S. port of entry (air, land, or sea). For ocean freight, an Importer Security Filing (ISF), also known as the "10+2 rule," must be transmitted to Customs and Border Patrol (CBP) at least 24 hours before the cargo is loaded onto the vessel to help CBP evaluate any risks. Once the vessel arrives, the importer receives a notice of arrival with details for pickup. CBP assesses the goods for compliance with U.S. import regulations.

The importer (or a licensed customs broker on their behalf) must file entry documents with CBP at the port of arrival within 15 calendar days of the shipment's arrival, usually through the Automated Commercial Environment (ACE) system. CBP may randomly select an imported shipment for inspection. Once the goods are cleared, the importer must file the entry-summary documentation and pay all estimated duties, taxes, and fees within 10 working days of the goods' release. We can expect increased enforcement to ensure that the country of origin of goods is true (transshipment actions), as well as to ensure that goods labeled as 'Made in America' were truly manufactured in the United States.

On the civil enforcement side, the FCA is the dominant statute utilized by the government. FCA matters can be self-generated by the government or come to the government via whistleblowers. On the criminal side, the government can invoke several statutes, including but not limited to false statements to a government agency (Section 1001), wire fraud, and general and specific conspiracy statutes. In the 2025 fiscal year, the Department of Justice reported that settlements and judgments under the False Claims Act exceeded $6.8 billion – the highest amount in a single year in the history of the Act.

Recent Matters

In March 2024, Akua Mosaics and its president pleaded guilty to conspiring to smuggle porcelain mosaic tiles by falsely labeling them as originating from Malaysia (when they were made in China), to avoid anti-dumping duties. They were sentenced (probation) and ordered to pay restitution of approximately $1.09 million. *United States v. Akua Mosaics*, No. 3:24-cr-00105-ADC (D.P.R.), ECF Nos. 38 & 39 (July 11, 2024).

In April 2025, DOJ intervened in *United States ex rel. Lee v. Barco Uniforms, Inc.* In this qui tam case, the Relator alleged that Barco conspired to undervalue imported apparel (from China) by misrepresenting values on invoices, thereby paying lower customs duties than required. *United States ex rel. Lee v. Barco Uniforms, Inc.*, No. 2:16-cv-01805-DC-JDP (E.D. Cal.), ECF No. 65 (April 11, 2025).

In July 2025, DOJ announced a $6.8 million settlement by Global Plastics LLC and Marco Polo International LLC, both subsidiaries of MGI International LLC, to resolve their civil liability under the FCA for knowingly failing to pay customs duties on certain plastic resin imported from China.

In July 2025, DOJ filed an FCA complaint (*United States ex rel. Joyce v. Global Office Furniture, LLC*) alleging that the company, Global Office Furniture, LLC, evaded at least $2 million in tariffs by submitting false (understated) invoices to U.S. Customs and Border Protection (CBP). *United States v. Global Office Furniture, LLC*, No. 2:20-cv-001223-DCN (D.S.C.), ECF No. 50 (July 15, 2025). The scheme involved "double-invoicing": one genuine invoice for the actual price (used to bill buyers), and a second, false, lower-value invoice submitted to CBP for calculating duties. The DOJ also claims that the executive directed the destruction of incriminating evidence (e.g., deleting emails). Id. at 17.

In July 2025, patio furniture company Grosfillex paid $4.9 million to resolve allegations made under the FCA that it evaded duties on extruded aluminum from China.

In September 2025, DOJ announced criminal charges against two Denver-area companies and the companies' top executives for defrauding the federal government on sales of forklifts and conspiring to avoid paying proper tariffs on forklifts imported into the United States.

Looking Ahead to 2026 and Beyond

Following the various DOJ announcements with respect to tariff enforcement and observing a consistent series of announcements in this case type, we expect to continue to see an uptake in this space.

- **Increased Use of FCA:** Many recent cases are civil, brought under the FCA. This suggests DOJ is leaning on whistleblower-driven enforcement to tackle customs fraud.
- **Criminal Enforcement:** While civil cases are prominent, there are still criminal prosecutions (e.g., the Akua Mosaics case), and DOJ has made "trade and customs fraud, including tariff evasion" a white collar enforcement priority.
- **Interagency Coordination:** The new task force formalizes cooperation between the Department of Homeland Security and DOJ—showing that the government is treating tariff evasion more systematically.
- **Transshipment Risk:** The CBP EAPA case (over $250 million in one probe) underscores the risk of illegal transshipment (routing goods through third countries to disguise origin) as a key method of evasion.

- **Whistleblower Incentives:** Given the use of FCA, the government is likely incentivizing insiders or competitors to report misdeeds; this could increase exposure for importers using aggressive or questionable classification / valuation strategies.

Clients should be extra diligent in ensuring the accuracy of whatever forms and representations are submitted to the government. We can expect increased enforcement to ensure that the country of origin for goods is accurately stated (to prevent transshipment), as well as to verify that products labeled 'Made in America' were truly manufactured in the United States.

HEALTH CARE AND FALSE CLAIMS ACT

By Matthew Ebert

Health care remained the focal point of federal FCA enforcement in 2025, with DOJ securing significant settlements, litigating high-stakes cases through verdict, and announcing expanded interagency enforcement priorities that will shape investigations in 2026.

Recent Matters

Several high-profile settlements underscored DOJ's continued focus on health care fraud:

- **Unlawful Kickbacks: Gilead Sciences (approximately $202 million)**
  Gilead resolved whistleblower allegations that it paid unlawful kickbacks to induce prescriptions of certain HIV medications, reinforcing DOJ's continued focus on pharmaceutical marketing and physician engagement practices. *United States, et al., ex rel. Bellman v. Gilead Sciences, Inc.*, No. 16-cv-6228-PAE (S.D.N.Y.), ECF No. 32 (April 30, 2025).
- **Medicare Advantage Risk Adjustment Settlements (approximately $62 million)**
  In March 2025, DOJ resolved allegations involving improper diagnosis coding and inflated risk scores submitted to Medicare Advantage plans, highlighting sustained enforcement attention on risk adjustment practices. *United States, et. al., ex rel. Pew v. Seoul Medical Group, Inc., et al.*, No. 2:20-cv-05156 (C.D. Cal.).
- **Improper Medical Device Reimbursement (approximately $37 million)**
  In September 2025, a device manufacturer and distributor settled claims that Medicare was billed for testing products for arterial disease that allegedly failed to meet program requirements.
  United States, et al., ex. rel. Kane v. Semler Scientific, Inc., No. 3:16-cv-1516 (M.D. Fla.).

Looking Ahead to 2026 and Beyond

On July 2, 2025, DOJ and the Department of Health and Human Services (HHS) formally renewed and expanded the DOJ-HHS False Claims Act Working Group, announcing enforcement priorities that will guide FCA referrals and investigations going forward into 2026 and beyond. The Working Group is designed to enhance data sharing, accelerate referrals, and coordinate enforcement across DOJ, HHS, and HHS-OIG.

Looking ahead to 2026, providers, payors, pharmacies, and life sciences companies should expect continued scrutiny across billing, coding, referral relationships, and compliance practices. Health care FCA enforcement in 2026 is expected to intensify in several key areas targeted by the DOJ-HHS False Claims Act Working Group:

- **Medicare Advantage**, including risk score inflation and unsupported diagnoses
- **Pharmacy benefit managers**, especially practices around rebates, pricing, and formulary decisions for drugs and devices
- **Kickbacks** involving drugs, devices, durable medical equipment, and other reimbursed items
- **Barriers to patients' access to care**, such as network adequacy violations

- **Materially defective medical devices** raising safety or efficacy concerns
- **Electronic health record manipulation**, including documentation practices used to justify medically unnecessary services

Clients in the health care space should assess compliance programs with these priorities in mind, focusing on coding accuracy, referral arrangements, pricing practices, and documentation integrity. The combination of large financial settlements, coordinated enforcement initiatives, and clearly articulated DOJ-HHS priorities signal that health care FCA risk remains high. Proactive compliance reviews and early issue identification will be critical as enforcement momentum carries into 2026.

WHISTLEBLOWER PROGRAMS

By Brad Gershel

Over the course of 2025, the enforcement framework for corporate misconduct evolved to place a premium on the role of the individual insider. While DOJ's Criminal (CRM) and Antitrust (ATR) Divisions, and the U.S. Attorney's Office for the Southern District of New York (SDNY), utilized different statutory tools rather than a single coordinated directive, their respective policy updates have converged on a similar outcome: the expansion of whistleblower leverage.

For company and outside counsel, these developments have introduced structural constraints into the internal investigation process. By establishing specific look-back periods for financial awards and distinct immunity channels for culpable individuals, the government has created incentives that often run counter to a company's preference for a deliberative, comprehensive review. The result is an environment where the timeline for assessing an allegation is increasingly dictated by the risk of an external report rather than the pace of factual development.

DOJ: The 120-Day Look-Back and the 'Minimal Participant' Exception

On May 12, 2025, the DOJ revised its *Corporate Whistleblower Awards Pilot Program*. While the program attracted attention for its financial incentives—awards up to 30 percent of the first $100 million in net proceeds forfeited—the DOJ introduced two structural changes that significantly increase the pressure on corporate compliance functions.

First, under Section II(2)(d) of the revised policy, the DOJ codified a "safe harbor" that allows a whistleblower to report misconduct internally and wait up to 120 days before contacting the DOJ, without losing their place in line. If the individual submits their information to the DOJ within that window, the DOJ "will deem the date the individual provided original information to the entity's internal reporting structure as the date of the individual's original disclosure to the Department." This establishes a retroactive priority system. By treating the date of the internal complaint as the effective date of the government report, the policy allows whistleblowers to secure "first-in" status based on when they made their internal report, not when they contacted the DOJ. By operation of the policy, a company that self-discloses months after an internal report—even if acting diligently—may find its disclosure rendered second-in-line by the whistleblower's retroactive priority date.

Second, the DOJ expanded the universe of potential whistleblowers to include individuals who were themselves implicated in the misconduct. While the program generally excludes individuals who meaningfully participated in the criminal activity, Footnote 4 introduces a critical exception for "minimal participants"—defined under U.S.S.G. § 3B1.2 as those "plainly among the least culpable of those involved in the conduct of a group." The policy explicitly links this financial eligibility to the CRM Division's separate *Pilot Program on Voluntary Self-Disclosures for Individuals*, noting that such individuals can potentially secure both a Non-Prosecution Agreement (NPA) *and* a financial award. This alignment creates a powerful dual incentive: a mid-level employee involved in a scheme now has a path to secure both their liberty and a financial award, effectively removing the self-incrimination barrier that has historically kept co-conspirators silent.

Antitrust Division: The Expansion of Financial Rewards

On May 7, 2025, the ATR Division moved to close a significant gap in its enforcement arsenal by establishing the *Whistleblower Rewards Program*. Historically, the ATR Division has lacked the direct statutory authority to pay awards, relying instead on its Corporate Leniency Policy (CLP), which grants immunity to the first corporation to self-disclose. Through a Memorandum of Understanding with the U.S. Postal Service (USPS), the ATR Division has now leveraged the USPS's existing authority under 39 U.S.C. § 2601 to pay rewards for information regarding Sherman Act violations that affect the mails or postal revenues.

While the program requires a nexus to the Postal Service, the MOU explicitly notes that the harm to the USPS "need not be material," effectively broadening the program's scope to cover a wide swath of "horizontal, 'per se' unlawful agreements, such as price fixing, bid rigging, and market allocation."

This initiative introduces a competing incentive structure to the CLP. Previously, a company's primary risk was that a co-conspirator would report first to secure immunity. Now, the risk is also internal. With the presumption of an award of "at least 15 percent of the recovered criminal fine" (capped at 30 percent), an employee aware of a cartel has a lucrative alternative to silence. Crucially, the program defines a voluntary submission as one made "before a formal demand (*e.g.*, grand jury subpoena)... is served." The practical result is a new, asymmetrical risk: an employee's independent financial interest in reporting can now trigger federal scrutiny well before the company has had the opportunity—or the inclination—to weigh the benefits of self-disclosure.

SDNY: Individual Immunity

Effective January 14, 2025, the SDNY implemented the *Whistleblower Non-Prosecution Pilot Program*. Unlike the DOJ program, which uses financial rewards to attract tips, the SDNY pilot incentivizes disclosure by offering an NPA to individuals who might otherwise face prosecution.

The program's eligibility criteria prioritize the timing of the disclosure. Condition 1 mandates that the "misconduct has not previously been made public and is not already known to SDNY or to any component of the DOJ." This establishes a zero-sum dynamic between the company and the individual. If the company investigates and self-discloses first, the individual loses their eligibility for an NPA. Conversely, if the individual reports first to secure their freedom, the company faces an investigation it did not initiate. This structure discourages culpable employees from reporting internally or waiting for an internal investigation to conclude; their only possible guarantee of immunity lies in beating the company to the prosecutor's office.

Additionally, the policy weaponizes corporate hierarchy to encourage reporting from the middle. Condition 5 explicitly disqualifies "the highest-ranking person within the organization" (such as the CEO or CFO) and anyone who "exercises primary control over the operations." By stripping senior leadership of eligibility, the SDNY creates a wedge between senior executives and their subordinates.

Looking Ahead to 2026 and Beyond

The policy updates of 2025 mark a distinct maturation in federal whistleblower enforcement. While external reporting channels are not new, the specific innovations of the past year—namely, the extension of financial eligibility to "minimal participants" and the SDNY's offer of total immunity to co-conspirators—have fundamentally altered the calculus for insiders. By creating a structured "race" that specifically targets those with potential criminal exposure, the government has effectively created a parallel track for employees that runs independently of, and potentially faster than, corporate governance.

For company and outside counsel, the practical consequence is a loss of exclusive control over the pacing of an investigation. In this environment, the challenge is to integrate the assessment of whistleblower risk directly into the initial scoping of an investigation. Rather than waiting for substantive corroboration of the underlying misconduct, counsel must make earlier judgments about the reporter's likely trajectory. The decision-making process regarding self-disclosure must move from a sequential model—investigate, then decide—to a concurrent one.

ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM, DIGITAL ASSETS, AND ARTIFICIAL INTELLIGENCE

By Katherine L. Oaks and Kelly A. Lenahan-Pfahlert

In 2025, the U.S. anti-money laundering (AML) and countering the financing of terrorism (CFT) landscape evolved with growing technological risks and federal policy increasingly focused on national security. Regulators are prioritizing threats of cybercrime, misuse of digital assets, and transnational criminal organizations, and emphasizing the value of AML tools in protecting national security. Financial institutions faced increased expectations for risk-based program design, data quality, and governance, amid a more complex supervisory landscape. Key developments in 2025—including new rules under the AML Act of 2020, expanded sanctions against cartels, digital asset regulation, and a focus on artificial intelligence fraud—signal continuing reliance on financial institutions to assist in guarding against threats to national security and exploitation of the U.S. financial system by a growing variety of criminal actors and methods into 2026.

AML/CFT

AML Developments: Heightened Focus on National Security and Centralized Enforcement

Key threats to the U.S. financial system that the Treasury identified in 2024—cybercrime, fraud, corruption, drug trafficking, and exploitation by foreign adversaries like North Korea—grew in priority in 2025. Federal agencies have increasingly applied this national-security lens to AML enforcement, with particular attention to cartels, transnational criminal organizations, Chinese money laundering networks (CMLNs), and sanctions-evasion schemes like Iranian shadow networks. Enforcement activity reflected a focus on targeted, intelligence-driven interventions.

In December, news outlets reported that Treasury will propose to significantly expand FinCEN's Bank Secrecy Act (BSA) and AML enforcement authority in 2026, which would make FinCEN the central decisionmaker in enforcement actions and give it the ability to override decisions by banking regulators. The proposal also envisions more intelligence-driven, risk-based enforcement that would prioritize actionable threats over technical compliance issues. Adoption would mean a significant change in AML enforcement, reshaping expectations for governance, escalation, and regulatory engagement.

Implementation of the AML Act. FinCEN advanced implementation of the AML Act of 2020, including a proposed rule that would require AML/CFT programs to be "effective, risk-based, and reasonably designed." The proposal would formalize expectations for enterprise-wide risk assessments, documented program-design decisions, and alignment of controls to identified risks.

Corporate Transparency Act (CTA). 2025 was the first full year of beneficial-ownership reporting under the CTA, during which Treasury and FinCEN continued to emphasize the importance of accurate and complete filings. The court in *National Small Business Association v. Yellen* held the CTA unconstitutional as applied to the plaintiffs, prompting FinCEN to pause enforcement only for those litigants and leaving reporting obligations unchanged for all other entities. However, the legal landscape shifted in December 2025, when the 11th Circuit upheld the constitutionality of the CTA, reducing the uncertainty created by earlier district court rulings. FinCEN's March 2025 interim final rule exempting most domestic U.S. entities from beneficial ownership reporting remained in effect, while foreign reporting companies continued to have BOI obligations.

Sector-specific rulemaking. FinCEN's long-pending AML program rule for investment advisers took a step forward on December 31, when FinCEN issued a final rule postponing the effective date of the investment adviser AML/CFT program and suspicious activity reporting requirements until January 1, 2028, confirming that the agency intended to revisit the rule's scope. Other rulemakings, relating to real estate, digital assets, and cross-border payments, remain under review.

Enforcement Reflects Policy of 'Total Elimination' of Cartels and TCOs That Threaten the U.S.

In January 2025, the president declared a federal policy of "total elimination" of cartels and transnational criminal organizations in Executive Order 14157 "Designating Cartels and Other Organizations as Foreign Terrorist Organizations and Specially Designated Global Terrorists."

In February, the State Department designated several cartels—primarily based in South or Central America—including the Sinaloa Cartel and Cartel de Jalisco Nueva Generacion (CJNG) as Foreign Terrorist Organizations (FTOs) and Specially Designated Global Terrorists (SDGTs).

In May, the Treasury's Office of Foreign Assets Control (OFAC) sanctioned two Mexico-based entities linked to the CJNG, associated with supporting a network generating millions for the cartel not only through drug trafficking, but also fuel theft and smuggling stolen crude oil into the U.S. Additional CJNG affiliates, including 13 Mexico-based companies, were sanctioned in August based on their links to CJNG timeshare fraud schemes that target U.S. tourists to generate revenue for the cartel.

In addition to tourism and oil, the directive to eliminate cartels threatening the U.S. led to sanctions touching other areas of legitimate commerce like agriculture. In August, OFAC sanctioned Carteles Unidos and Los Viagras, based in part on extortion in the agriculture industry.

FinCEN issued orders in June identifying three financial institutions based in Mexico—CIBanco S.A., Institución de Banca Multiple (CIBanco), Intercam Banco S.A., Institución de Banca Multiple (Intercam), and Vector Casa de Bolsa, S.A. de C.V. (Vector)—as "primary money laundering concerns" and prohibiting certain transmittals of funds involving them. These were FinCEN's first actions under the Fentanyl Sanctions Act and the Fentanyl Eradication and Narcotics Deterrence (FEND) Off Fentanyl Act, passed in 2024 to strengthen U.S. agencies' powers to target money laundering associated with narcotics trafficking.

FinCEN has also raised the alarm on the threat CMLNs pose to the U.S. financial system, urging particular vigilance by financial institutions to detect use of CMLNs by Mexico-based cartels, including those designated as FTOs. The agency highlighted the speed and effectiveness of CMLN operations, and the various methods CMLNs use to launder proceeds for cartels, including through shell companies investing in the U.S. real estate market.

While sanctions primarily serve as a tool to influence behavior rather than to punish— such as disrupting money laundering networks and transnational criminal activities—Treasury has warned it will use its powers to impose secondary sanctions on financial institutions facilitating transactions with designated entities, imposing civil or criminal penalties on U.S. and foreign persons, and restricting or prohibiting U.S. correspondent accounts.

Conducting business internationally and particularly in Mexico and South America, for financial institutions as well as any companies involved in oil, agriculture, tourism, or other industries, will require sharpened vigilance through 2026. This will mean heightened diligence and review of compliance programs, as well as staying abreast of a rapidly evolving federal landscape of AML/CFT enforcement and as digital assets regulations are rolled out under the Guiding and Establishing National Innovation for US Stablecoins Act (GENIUS Act).

Digital Assets

Regulatory Focus: Protect Investors, Make U.S. 'Crypto Capital of the Planet'

In January 2025, President Trump signed Executive Order 14178 "Strengthening American Leadership in Digital Financial Technology," signaling a shift away from regulation toward growth of digital financial technology in the U.S. According to President Trump, Executive Order 14178 is a step in fulfilling his promise to make the U.S. "the crypto capital of the planet." The executive order creates a Presidential Working Group on Digital Asset Markets to develop a federal regulatory framework for digital assets, prohibits agency efforts to establish central bank digital currencies, and revoked Executive Order 14067 "Ensuring Responsible Development of Digital Assets" (March 9, 2022) and the U.S. Treasury's Framework for International Engagement on Digital Assets (July 7, 2022).

The most significant congressional act in 2025 impacting digital assets was the passage of the GENIUS Act in July. The first-ever U.S. digital assets law creates a regulatory framework for dollar-backed stablecoins, with requirements for issuer permitting, reserves, and AML controls, and will go into effect in 2027.

At DOJ, the focus shifted sharply away from "regulating by prosecution" to targeting conduct that victimizes U.S. investors or supports cartels based in South America and Mexico. In an April 7 Memo "Ending Regulation by Prosecution," DOJ announced it would shift enforcement to focus on prosecuting conduct victimizing investors, consistent with Executive Order 14178, and use of digital assets to further unlawful conduct by cartels, TCOs, FTOs, and Specially Designated Global Terrorists, in line with the "total elimination" policy laid out in Executive Order 14157. DOJ indicated it would pursue illicit financing of fentanyl and human trafficking, terrorism, cartels, and smuggling, including through use of digital assets, but it would not take action against platforms used for these activities.

For example, DOJ's Criminal Division launched the Scam Center Strike Force, partnering with the D.C. U.S. Attorney's Office, the FBI, and the Secret Service, to investigate "scam compounds" in Southeast Asia through which Chinese transnational criminal organizations defraud Americans of billions annually through cryptocurrency investment scams and related fraud schemes. OFAC and FinCEN have supported this effort as well, in collaboration with international allies like the U.K. OFAC designated several companies in Cambodia and Burma in May and September for involvement in operating scam compounds targeting Americans through cyber scams, and in a sweeping action in October, coordinated with the U.K. to sanction the Cambodia-based Prince Group for online investment scams targeting Americans and others. FinCEN imposed a special measure in October prohibiting U.S. financial institutions from opening or maintaining correspondent accounts for Cambodia-based financial institution Huione Group, deemed a primary money laundering concern under § 311 of the Patriot Act, and requiring special due diligence on foreign correspondent accounts to guard against the threat.

OFAC actions in 2025 more broadly reflect alignment with the policy to protect investors and disrupt cybercrime networks that fund actors considered a threat to U.S. national security. In March, OFAC removed economic sanctions from the digital assets intermediary and cryptocurrency mixer Tornado Cash, in response to the Fifth Circuit's 2024 ruling in *Van Loon v. Department of the Treasury* that OFAC lacked IEEPA authority to sanction open-source code. The agency made clear it remains focused on those considered a threat to security and U.S. leadership in the digital asset industry, a reference to its rationale for the sanctions: that Tornado Cash aided criminal actors, including North Korea's state-funded hacking organization the Lazarus Group, in laundering billions. In November, OFAC imposed sanctions specifically targeting cybercrime and money laundering activities funding North Korea's nuclear weapons program, on two entities and eight individuals linked to cybercrime and IT worker fraud schemes supporting North Korea.

DOJ saw its prosecution of Tornado Cash co-founder Roman Storm through in 2025, securing his conviction in August of knowingly transmitting criminal proceeds over the platform. In another digital assets case, the founders of cryptocurrency mixing service Samourai Wallet were sentenced to four and five years in prison for knowingly transmitting $237 million in criminal proceeds. The two cases signal DOJ's continued focus on willful actions and individual actors, and a shift away from 'regulating' technology and services through prosecution.

OFAC also increased pressure on the Iranian shadow fleet and laundering network, used to evade sanctions and finance Iran's nuclear program, imposing new sanctions on 29 fleet vessels and their management firms in December. FinCEN's October analysis identifying approximately $9 billion in Iranian shadow banking activity occurring through U.S. correspondent accounts highlighted particular vulnerabilities to the network and need for heightened diligence.

At the Securities and Exchange Commission (SEC), the 2025 trend has also been one of deregulation. In January, SEC formed a Crypto Task Force to help develop a clear regulatory framework for crypto assets and increase transparency and public engagement in developing crypto policy. In February, SEC cited its focal shift to reform in dismissing its enforcement action against Coinbase Inc., which had alleged the company operated as an unregistered securities exchange, broker, and clearing agency by listing and facilitating trade of certain crypto tokens. SEC explained the dismissal was based on policy and not reflective of its view of the merits. This is a clear shift from last year's SEC, which pursued Terraform Labs and founder Do Kwon to verdict for selling the TerraUSD stablecoin and LUNA token without registration in violation of U.S. securities laws.

Artificial Intelligence

Regulators in 2025 also intensified focus on AI as a technological force reshaping the AML landscape, building on the uses, opportunities, and risks the Treasury highlighted in December 2024, including that AI and generative tools can strengthen risk management but also present risks of data quality, bias, explainability, and third-party dependencies. Regulators focused on AI-enabled illicit finance and the need for controls to reflect evolving typologies, model governance and explainability, data quality and lineage, operational resilience and bias mitigation, and use of AI to detect complex illicit activity. AI is also a resource to enhance AML/CFT programs, provided institutions apply disciplined governance and align AI use with risk-based program design.

AI Deepfakes and Fraud. FinCEN also warned of a rise in deepfake-enabled fraud heading into 2025, including synthetic voices, fabricated identities, manipulated documents, and realistic video impersonations used to bypass identity verification and authentication controls. These techniques facilitate account takeovers, social engineering schemes, and large-scale financial fraud. Enforcement agencies also note increasing use of deepfakes to impersonate both customers and employees, warning that these schemes have become more scalable and difficult to detect.

Given the unique risks posed by AI, FinCEN calls for strengthening controls across onboarding, authentication, and monitoring. Specifically, through enhanced identity-verification measures, monitoring for synthetic identities, integration of deepfake typologies into risk assessments, and rigorous testing and governance of AI-based detection tools. Institutions are also encouraged to participate in public-private information-sharing to support early detection.

Looking Ahead to 2026 and Beyond

The past year highlighted the growing use of AML and sanctions tools for national security interests, and an overarching policy in combating financial crime that harms U.S. investors, exploits the U.S. financial system, or supports cartels, transnational criminal organizations, and other actors adverse to the U.S., like North Korea and Iran. While deregulation is a trend in this area, financial institutions should remain vigilant and abreast of compliance requirements in a quickly evolving technological and regulatory space. In 2026, institutions should anticipate:

- **Expanded involvement of FinCEN in AML enforcement:** Treasury's proposal to expand FinCEN's authority may reshape interagency roles, leading to faster intervention in high-risk matters, and heightened scrutiny of governance and escalation practices.
- **Increased focus of AML and sanctions enforcement on national security:** Agencies will continue prioritizing threats tied to cartels, CMLNs, foreign adversaries, and cyber-enabled activity. Institutions with cross-border exposure—particularly in Mexico, South America, and other high-risk sectors—should anticipate expanded due diligence expectations and increased use of secondary sanctions and § 311-style measures.
- **Total elimination of cartels and TCOs means staying abreast of trends in cartel revenue streams and terrorist financing:** The growing variety of cartel revenue sources will demand greater due diligence and monitoring relating to legitimate commerce—agriculture, tourism, real estate, weapons, and oil, particularly in high-risk areas.

- **Stricter requirements for AI governance and deepfakes resilience:** Regulators will intensify focus on AI governance, data quality, explainability, and controls to detect AI-enabled fraud, synthetic identities, and deepfake-driven account takeovers.
- **Digital assets regulation:** Institutions should stay tuned for the roll out of regulations under the GENIUS Act, as regulators prepare to implement the law when it takes effect in 2027.

Financial institutions that invest in robust controls and readily adapt to evolving regulations (investment adviser rules, real estate transparency, cross-border transactions, and digital assets), sanctions, and geopolitical trends will best navigate the quickly shifting federal AML/CFT environment in 2026.

CONCLUSION

The ever-changing environment of white collar defense and internal investigations demands vigilance and proactive strategies from organizations operating in today's high-stakes regulatory climate. As enforcement actions increase in areas such as tariffs and customs, FCA matters, whistleblower claims, money laundering, cartels, cryptocurrency regulation, and artificial intelligence oversight, it is critical for companies to stay informed and prepared.

The attorneys in Ballard Spahr's White Collar Defense and Investigations Group have extensive experience guiding clients through these complex issues and can provide strategic counsel on all aspects of criminal investigations and defense.

CONTACTS

HENRY E. HOCKEIMER, JR.
Partner and Practice Group Leader, White Collar Defense and Investigations
Philadelphia
hockeimerh@ballardspahr.com
215.864.8204

MARJORIE J. PEERCE
Senior Counsel, White Collar Defense and Investigations
New York
peercem@ballardspahr.com
646.346.8039

MATTHEW EBERT
Counsel, White Collar Defense and Investigations
Minneapolis
ebertm@ballardspahr.com
612.371.2418

BRAD GERSHEL
Counsel, White Collar Defense and Investigations
New York
gershelb@ballardspahr.com
646.346.8034

KATHERINE L. OAKS
Associate, White Collar Defense and Investigations
Philadelphia
oaksk@ballardspahr.com
215.864.8263

KELLY A. LENAHAN-PFAHLERT
Senior Staff Attorney, White Collar Defense and Investigations
Philadelphia
lenahanpfahlertk@ballardspahr.com
215.861.7311

WILSON SMERCONISH
Associate, White Collar Defense and Investigations
Philadelphia
smerconishw@ballardspahr.com
215.864.8414