Clifford Chance

BRIEFING

Financial Crime Enforcement:

Key Issues to Watch in the United States in 2026

January 2026

The United States is at a major turning point in financial crime enforcement. Sweeping policy shifts, resource realignments, and new enforcement priorities under the Trump administration have refocused attention on national security threats, high-impact fraud, and cross-border criminal networks. With recalibrated approaches to corporate self-disclosure, whistleblower incentives, and digital assets, US authorities are targeting sectors and conduct that pose the greatest risk to American interests.

Key takeaways

1 **Refocused Enforcement Priorities and Sectoral Scrutiny**

2025 brought a significant realignment of US financial crime enforcement priorities. The DOJ, after staff reductions and policy changes, prioritised action against cartels, transnational criminal organisations, and foreign terrorist groups (FTOs). Sectors tied to national security – such as infrastructure, defence, energy, and government contracting – faced greater scrutiny, especially where US interests or fair competition were at stake. The DOJ's new plan targets high-impact cases with a strong US connection, with less emphasis on minor breaches.

2 **Corporate Self-Disclosure, Whistleblower Incentives, and Enforcement Efficiency**

The DOJ's updated policies now offer clearer incentives for voluntary self-disclosure and cooperation. Companies that promptly report and address misconduct are more likely to receive declinations or non-prosecution agreements, even in serious cases. The DOJ has limited the use of corporate monitorships, favouring shorter, targeted investigations and early resolution. Whistleblower protections and rewards have also been expanded, encouraging reports of a wider range of misconduct.

3 **Regulatory Developments and Digital Assets**

US regulators have adjusted their approach to digital assets. The DOJ now focuses on fraud, money laundering, and criminal use of cryptocurrencies, rather than technical breaches. The Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) are working to clarify the regulatory perimeter for digital assets, with new proposals aiming to reduce uncertainty. Enforcement now targets conduct posing real risks to investors or the financial system, with strong action against scams and illicit activity.

ENFORCEMENT TRENDS

What have been the most significant developments in financial crime enforcement in the US in 2025?

In the first half of 2025, the Trump administration transformed financial crime enforcement. Through the actions of the Department of Government Efficiency (DOGE) and the Trump administration's deferred resignation program, the DOJ lost more than 4,000 employees. The DOJ also scaled down a number of units dedicated to financial crime enforcement, including dramatically reducing the number of attorneys assigned to the Public Integrity Section and disbanding Task Force KleptoCapture. At the same time, President Trump's own appointees announced new priorities, including redirecting resources to focus on cartels and TCOs.

In February, the Trump administration issued an Executive Order announcing a "pause" on new Foreign Corrupt Practices Act (FCPA) investigations (the February Executive Order), which was subsequently ended in June when the DOJ confirmed that FCPA enforcement would resume pursuant to new enforcement guidelines. Elsewhere, the SEC dismissed or closed enforcement actions from the prior administration, including one of the last remaining crypto enforcement actions brought against a major cryptocurrency exchange.

In May, the DOJ's Criminal Division announced significant changes to its Corporate Enforcement and Voluntary Self-Disclosure Policy, Memorandum on Selection of Monitors in Criminal Division Matters, and Corporate Whistleblower Awards Pilot Program, and further clarified its future enforcement priorities, in the form of a memorandum outlining the DOJ's White-Collar Enforcement Plan. For a more detailed analysis of these recent developments, see the Clifford Chance blogs here, here, here, and below.

The SEC has recently undergone a period of significant leadership transition, marked by a series of high-profile senior appointments and departures that are likely to shape the agency's regulatory priorities and enforcement strategy. In April, Paul Atkins was appointed by President Trump as Chairman of the SEC. Since his appointment, Mr Atkins has stated that the SEC would adopt a less aggressive enforcement approach, strongly criticizing the former approach taken within the SEC, which he viewed as overly formulaic and draconian.

In September, Judge Margaret Ryan was named Director of the Division of Enforcement, with Sam Waldon, Acting Director of Enforcement, returning

to his previous role as Counsel for the Division. More recently, in December, SEC deputy enforcement director Antonia Apps stepped down after a short tenure marked by broad changes in enforcement priorities at the agency. Under Judge Ryan's leadership, SEC enforcement will continue to shift away from the aggressive use of novel legal theories and become more structured and predictable.

Looking ahead to 2026, the Trump administration announced in an 8 January fact sheet plans to establish a new Department of Justice 'National Fraud Enforcement' division, to be led by a newly appointed Assistant Attorney General. This division would be responsible for coordinating both civil and criminal enforcement actions against fraud affecting federal programmes, federally funded benefits, businesses, non-profits, and private individuals. The White House has presented this initiative as a response to what it describes as “rampant” fraud, signaling a likely increase in the administration’s focus on fraud enforcement. This development follows the DOJ’s abolition of its tax division late last year, with its functions transferred to the criminal and civil divisions – a move intended to improve departmental efficiency.

How did the DOJ's enforcement priorities shift in May 2025?

The DOJ's White-Collar Enforcement Plan outlined ten "high-impact areas" that the DOJ “will prioritize investigating and prosecuting". The focus areas include various forms of fraud and misconduct that harm public and US interests including healthcare and federal program fraud, trade and customs fraud, and fraud through variable interest entities (primarily targeting Chinese-linked companies listed on US stock exchanges), such as securities fraud and Ponzi schemes.

Enforcement efforts targeting national security threats involving financial institutions that facilitate transactions for cartels and terrorist organizations are expected to increase. There will also be a heightened focus on corporate support for FTOs, complex money laundering schemes, offences related to controlled substances and counterfeit drugs, and bribery that undermines US interests. Additionally, crimes involving digital assets, especially those victimizing investors or facilitating other criminal activities, are set to be prioritized, particularly cases involving cartels, TCOs, or terrorist groups.

The DOJ also committed to greater transparency in enforcement procedures, and a reduction in the burden of lengthy investigations on US businesses by promoting shorter, more targeted inquiries, allowing for early termination of corporate resolutions when suitable. The revised policies have enhanced the benefits of self-disclosure, offering clearer paths to declinations and increased access to non-prosecution agreements, even in cases with aggravating factors. Additionally, the DOJ has indicated that monitorships will be limited to situations where benefits outweigh costs and expanded the DOJ Corporate Whistleblower Awards Program (first piloted in August 2024) to cover a wider range of fraud and misconduct (see further details below).

How did the DOJ clarify its enforcement priorities throughout the remainder of 2025?

The DOJ has clarified its enforcement priorities through a series of policy statements and practical actions in 2025, signaling a more targeted and

interest-driven approach to Foreign Corrupt Practices Act (FCPA) enforcement. In June, the DOJ issued new Guidelines for Investigations and Enforcement of the Foreign Corrupt Practices Act (FCPA). These Guidelines, together with remarks from the DOJ's leadership, signaled a decisive end to the FCPA "pause" and set out a more targeted, interest-driven approach to FCPA enforcement. The DOJ made clear that future FCPA investigations and enforcement actions will be governed by four core principles derived from the February Executive Order: (1) prioritizing cases involving cartels, TCOs, and FTOs; (2) safeguarding fair opportunities for US companies by focusing on misconduct that deprives American entities of fair competition or causes them economic harm; (3) advancing US national security, with particular attention to threats involving sectors such as defense, intelligence and critical infrastructure; and (4) concentrating resources on serious misconduct, rather than minor or customary business practices.

The Guidelines also introduced additional limiting principles, including a focus on individual misconduct, expeditious investigations, and consideration of the collateral consequences for companies and employees. DOJ officials emphasized that enforcement would be reserved for conduct that genuinely impacts US interests, with cases lacking such a nexus to be left to foreign authorities. Further, the DOJ reiterated its commitment to prosecutorial efficiency, transparency, and the prioritization of self-disclosure, while narrowing the use of monitorships and reinforcing the importance of robust corporate compliance programs.

Recent enforcement actions have demonstrated the DOJ's application of these clarified priorities. In August, the DOJ unsealed the first FCPA indictment charging two Texas-based Mexican businessmen with violations of the FCPA for their alleged role in a bribery scheme to retain and obtain business related to Petróleos Mexicanos (PEMEX), Mexico's state oil company. One defendant's trial concluded in December, with guilty verdicts for violating and conspiring to violate the FCPA.

In October, Smartmatic, a UK-based voting machine company, was charged in a superseding indictment with conspiracy to violate the FCPA and conspiracy to commit money laundering. The indictment alleges that Smartmatic and its executives paid over US$1 million in bribes to the former chairman of the Republic of the Philippines' Commission on Elections to secure contracts to provide voting machines and election services for the country's 2016 elections. The company has pleaded not guilty and is currently engaged in proceedings in court. FCPA charges against companies are relatively rare, as most companies prefer to resolve matters pre-indictment – this development therefore highlights the DOJ's focus on both individual and corporate accountability, even where the company has cooperated with authorities.

Separately, the trial of former coal executive Charles Hunter Hobson is set to proceed in early 2026. Hobson was arrested in 2022 on charges of violating the FCPA, laundering funds, and allegedly receiving kickbacks as part of an alleged scheme to bribe Egyptian officials to secure over US$143 million in contracts for Pennsylvania-based Corsa Coal from an Egyptian state-owned and state-controlled company, Al Nasr Company for Coke and Chemicals.

SECTORS AND TARGET INSTITUTIONS IN FINANCIAL CRIME INVESTIGATIONS

Which sectors have faced increased scrutiny for financial crime in 2025?

Under the DOJ's FCPA Guidelines, companies operating in high-risk sectors, particularly those linked to US national security interests such as critical infrastructure, defense, and natural resources, have faced heightened scrutiny. The February Executive Order specifically identifies areas such as critical minerals, deep-water ports, and other essential infrastructure or assets. Additional sectors that may also attract increased attention include advanced semiconductor manufacturing, telecommunications networks, energy generation and distribution facilities, water treatment plants, and major transportation hubs.

In September, the SEC and the CFTC announced a new, coordinated approach to enforcement aimed at reducing regulatory overlap and inconsistencies between the two agencies. Both the SEC and CFTC have expressed a renewed commitment to working together to take action against financial institutions involved in straightforward cases of fraud and insider trading, including misconduct by members of ad hoc creditors' committees.

Financial institutions and their insiders involved in sanctions violations or facilitating transactions with cartels, TCOs, hostile nation-states, and/or FTOs have also been identified as potential enforcement targets. Digital asset financial service providers – including cryptocurrency exchanges, tumblers, and mixers – associated with cartels, TCOs, or terrorist groups, or those facilitating drug money laundering or sanctions evasion, are further set to receive the "highest priority" from the DOJ.

Sectors involved in government contracting, healthcare (including Medicare and Medicaid programs), and customs have faced increased scrutiny from the DOJ for potential False Claims Act (FCA) violations. In March, a company, its subsidiary, and their former president and majority owner paid over US$62 million to settle FCA claims relating to the submission of false diagnosis codes to increase payments from the Medicare Advantage program. Further, in July, the DOJ and Department of Health and Human Services announced the relaunch of the False Claims Act Working Group to prioritize enforcement in this sector, signaling a more coordinated approach to enforcement in the healthcare sector.

Chemicals and equipment manufacturers in industries linked to the unlawful distribution of opioids continue to face increased enforcement action under the Controlled Substances Act (CSA) and the Federal Food, Drug and Cosmetic Act (FD&C Act). The DOJ in April announced an up to US$350 million settlement with a major pharmacy store chain to resolve allegations of illegally filling millions of invalid prescriptions for opioids and other controlled substances in violation of the CSA and then sought payment for many of those invalid prescriptions from Medicare and other federal health care programs in violation of the FCA. Importers have also faced heightened enforcement and compliance due to the introduction of a cross-agency Trade Fraud Task Force by the DOJ, in partnership with the Department of Homeland Security. The Task Force is designed to bring robust enforcement against importers and other parties seeking to defraud the US by evading tariffs, duties, or importing prohibited goods.

The initiative is part of the Administration's "America First" Trade Policy and emphasizes that enforcement efforts will target conduct that undermines US manufacturers, threatens domestic industries, and weakens national security.

FINANCIAL CRIME TRIGGERS, WHISTLEBLOWERS AND CORPORATE SELF-DISCLOSURE

What are the common key sources and triggers for the investigation of financial crimes in the US?

Common triggers for financial crime investigations in the US remain suspicious activity reports (SARs), whistleblower disclosures (most notably, FCA, SEC, CFTC, FinCEN, Internal Revenue Service and expanded DOJ whistleblower programs), and anomalies detected through transaction monitoring systems. Regulatory alerts and media investigations increasingly play a role. For example, FinCEN's alerts on fentanyl and oil smuggling have led to increased SAR filings, prompting investigations.

Data analytics is also being used by the SEC to quickly detect and successfully enforce insider trading cases. Additionally, the growing incorporation of artificial intelligence (AI) and machine learning in compliance systems has enhanced the detection of money laundering activities, such as layering and structuring, reducing the number of false positives. However, the use of advanced AI tools also introduces new risks, such as the potential for erroneous AI-initiated whistleblowing disclosures to regulators or the media – an issue likely to face increasing scrutiny in 2026 and beyond.

Given the international dimension of financial crimes and regulatory investigations, investigations are likely to change in frequency in accordance with the US's international trade policy, and as greater scrutiny is placed on jurisdictions of interest. Of particular note in 2025:

(a) In April, a bill was introduced with bipartisan support in the U.S. Senate seeking to investigate Hong Kong's alleged role in facilitating "money laundering and violations of export controls and sanctions." This came following escalating US-China trade tensions. More recently, in November, the DOJ charged four men for allegedly using US-based companies as a front to purchase and illegally export hundreds of computer components to China.

(b) In October, a former DOJ official cautioned that aggressive enforcement is expected against companies with potential ties to Latin American cartels, particularly given the Trump administration's greater focus on TCOs originating from that region.

(c) In November, the DOJ charged an Indonesian jewelry company and its employees with an alleged scheme to dodge more than US$86 million in US tariffs and duties, which came amidst the Trump administration imposing hefty tariffs on countries around the world in an aggressive bid to renegotiate more beneficial trade deals.

What has been the impact of the May 2025 legislative changes expanding whistleblower protections?

In May 2025, the DOJ revised its Corporate Whistleblower Awards Program, significantly broadening the scope of misconduct covered to include procurement fraud, trade, tariff and customs fraud, as well as offences related to sanctions, terrorism, cartels, and transnational criminal organizations. Whistleblowers are now eligible for substantial financial rewards if their information leads to asset forfeitures exceeding US$1 million, with awards of up to 30% of the first US$100 million and 5% of amounts between US$100 million and US$500 million.

The FinCEN AML Whistleblower Program, under the Anti-Money Laundering Act of 2020, continues to offer 10–30% rewards for actionable tips resulting in sanctions over US$1 million, supported by a US$300 million revolving award fund. Additional funding allocated in 2025 is expected to enhance FinCEN's capacity to manage the program and improve information-sharing with law enforcement partners.

Looking ahead, if the Federal Trade Commission (FTC) Whistleblower Award Program Bill is passed, it will further expand protections and incentives for whistleblowers reporting violations of federal consumer protection and antitrust laws. The proposed program, modelled on the SEC Whistleblower Program, would allow eligible whistleblowers to receive 10–30% of funds collected by the government as a result of their disclosures.

What recent developments have there been in the DOJ's approach to corporate self-disclosure and resolution of financial crime matters, and how have these shaped enforcement outcomes?

The DOJ's revised Corporate Enforcement and Voluntary Self-Disclosure Policy now provides a clearer route to declinations. Companies that voluntarily self-disclose misconduct to the DOJ, fully cooperate with investigations, and remediate the misconduct promptly and appropriately – provided there are no aggravating factors, such as the seriousness or pervasiveness of the offense, significant harm caused, or recent similar criminal conduct by the company – will, according to the DOJ, "receive a declination, not just a presumption of a declination."

The Head of the DOJ's Criminal Division, Matthew Galeotti, in comments made over the summer that the revised policy has narrowed the definition of aggravating factors, offering greater transparency and certainty for companies considering self-reporting, and the Criminal Division is concluding its review of all corporate monitors and has already terminated some. He has emphasized that monitors are intended as a "temporary bridge and accountability measure to move a company quickly and efficiently to full compliance", rather than a permanent requirement. Galeotti also recently noted that the DOJ would take on a much more active role in overseeing compliance in place of a monitor.

The policy expands access to Non-Prosecution Agreements (NPAs) for companies that make good faith but delayed, self-disclosures – even if the DOJ is already aware of the conduct. Eligible companies may receive an NPA with a term of less than three years, a 75% reduction in the criminal fine, and no monitorship. To qualify, companies must promptly disclose all relevant facts and individuals involved, provide access to documents and witnesses, and remediate based on a "root cause analysis."

In August, a global insurance company received a declination of prosecution despite reported evidence of FCPA violations. The DOJ cited the company's timely and voluntary self-disclosure, its full and proactive cooperation, the nature and seriousness of the offence, the timely and appropriate remediation, the significant improvements made to its compliance program, the absence of aggravating factors, and the agreement to disgorge approximately US$4.7 million.

Similarly, in September, it was announced that a major American Investment bank had settled with the DOJ after voluntarily self-disclosing spoofing schemes orchestrated by two former traders, pursuant to which the bank agreed to disgorge US$1.96 million and pay US$3.6 million into a victim compensation fund, while the DOJ declined to prosecute.

EMERGING RISK MANAGEMENT ISSUES

How did U.S. regulatory bodies address financial crime risks associated with cryptocurrencies and other digital assets in 2025?

In 2025, U.S. regulators recalibrated their approach to digital assets, with President Trump signaling a strong pro-digital assets stance. In April, Deputy Attorney General Todd Blanche issued a memorandum to all employees of the DOJ asserting that the DOJ will no longer pursue actions imposing regulatory frameworks on digital assets. Prosecutors were advised not to charge regulatory violations in digital asset cases unless they are knowing and willful, focusing instead on prosecuting individuals who exploit digital asset investors or use digital assets for criminal activities.

During the course of the year, SEC Chair Paul Atkins further announced that the agency is progressing towards proposing cryptocurrency regulations, with the SEC's Crypto Task Force expected to complete key work within months. In his Keynote Address at the Crypto Task Force Roundtable on Tokenization in May, Mr Atkins outlined the framework's goal to clarify the issuance, custody, and trading of crypto assets while deterring fraud. He emphasized the need to adapt regulations for the shift from traditional to blockchain-based systems, likening it to the music industry's digital transformation.

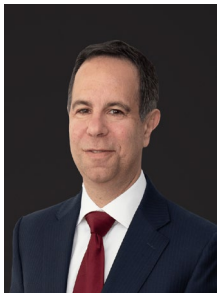
In November, Mr Atkins pledged to "draw clear lines" to provide greater clarity regarding the scope of its authority over the regulation of crypto transactions. The Commission is developing a "token taxonomy" which includes distinguishing between investment contracts (which may be securities) and other digital assets such as commodities, collectibles, or utility tokens, which may fall outside the SEC's jurisdiction. The SEC is also working on tailored exemptions and offering regimes for certain tokens, while making clear that enforcement will remain robust against fraudulent or deceptive conduct.

The CFTC is preparing to oversee spot trading of digital commodities and is working with the SEC to avoid conflicting rules, especially for hybrid digital assets. Congress is considering major legislation, including the GENIUS Act, which creates a regulatory framework for stablecoins to address consumer protection and risk. The separate CLARITY Act aims to clarify whether digital assets are regulated by the SEC or CFTC, reducing

uncertainty and enforcement risk for market participants. Additionally, the House has passed the Anti-CBDC Surveillance State Act, which restricts the Federal Reserve from offering products or services directly to individuals, maintaining accounts on their behalf, or issuing a central bank digital currency (CBDC), such as a digital dollar. The Act also prohibits the Federal Reserve's Board of Governors from using a CBDC to implement monetary policy, or from testing, studying, creating, or implementing a CBDC, except in circumstances specifically permitted by the bill.

This past year also saw the SEC establish the Cyber and Emerging Technologies Unit (CETU) to replace the Crypto Assets and Cyber Unit, with a focus on protecting retail investors who may be the victims of cyber and related frauds. The SEC's Division of Trading and Markets and the CFTC's Division of Market Oversight and Division of Clearing and Risk have announced a cross-agency initiative in furtherance of the SEC's Project Crypto and the CFTC's Crypto Sprint to coordinate efforts regarding the process for enabling the trading of certain spot crypto asset products.

US authorities have intensified enforcement against cryptocurrency investment scams run by transnational criminal organizations, launching the Scam Center Strike Force – a multiagency effort targeting "pig butchering" scams (i.e. scams in which victims are unwittingly targeted and defrauded over a period of weeks or months) in Southeast Asia. The Strike Force is already operational and has seized over US$401 million in fraudulent crypto assets.



Glen Donath
Partner, Washington DC

Email: glen.donath@cliffordchance.com
Mobile: +1 202 912 5138

Erica Lignell
Associate, New York

Email: Erica.Lignell@CliffordChance.com
Mobile: +1 212 878 8158

Robert-Arthur Yick
Associate, Washington DC

Email: robert-arthur.yick
@cliffordchance.com
Mobile: +1 202 912 5927