BSA/AML, SANCTIONS & EXPORT CONTROLS ENFORCEMENT AND COMPLIANCE ANNUAL UPDATE

February 4, 2026

Joint Presentation by the Anti-Money Laundering,
International Trade, Sanctions and Export Enforcement, and
National Security Practice Groups of Gibson Dunn

GIBSON DUNN

MCLE Credit Information

- Approved for 2.0 hours General PP credit in NY, CA, and CT.
- Approved for 2.0 CPD Credit by Solicitors Regulation Authority.
- Approval pending for 2.0 hours General PP Credit in CO, IL, TX, VA, and WA.
- CLE credit form must be submitted using the below link by **Wednesday, February 11th**. The announced CLE Codes will need to be entered in the form.
- Form Link: https://gibsondunn.qualtrics.com/jfe/form/SV_eDHuohAXeyXfMbQ
- Most participants should anticipate receiving their certificate of attendance in four to eight weeks following the webcast.
- Please direct all questions regarding MCLE to CLE@gibsondunn.com.

Our Speakers

Matthew S. Axelrod
Partner / Washington, D.C.

Stephanie L. Brooker
Partner / Washington, D.C.

David P. Burns
Partner / Washington, D.C.

Ella Alves Capone
Of Counsel / Washington, D.C.

M. Kendall Day
Partner / Washington, D.C.

Sam Raymond
Of Counsel / New York

Samantha Sewall
Of Counsel / Washington, D.C.

F. Joseph Warin
Partner / Washington, D.C.

TABLE OF CONTENTS

Overview of Regulatory Landscape

01

U.S. AML, Sanctions, and Export Regulators and Enforcers

Primary AML, Sanctions, and Export Regulators

FinCEN

State Regulators

OFAC

BIS

Secondary AML and Sanctions Regulators

Banking Regulators (OCC, Fed, FDIC, NCUA)

CFTC

SEC

FINRA

Enforcers

DOJ Criminal Division

Money Laundering, Narcotics and Forfeiture Section

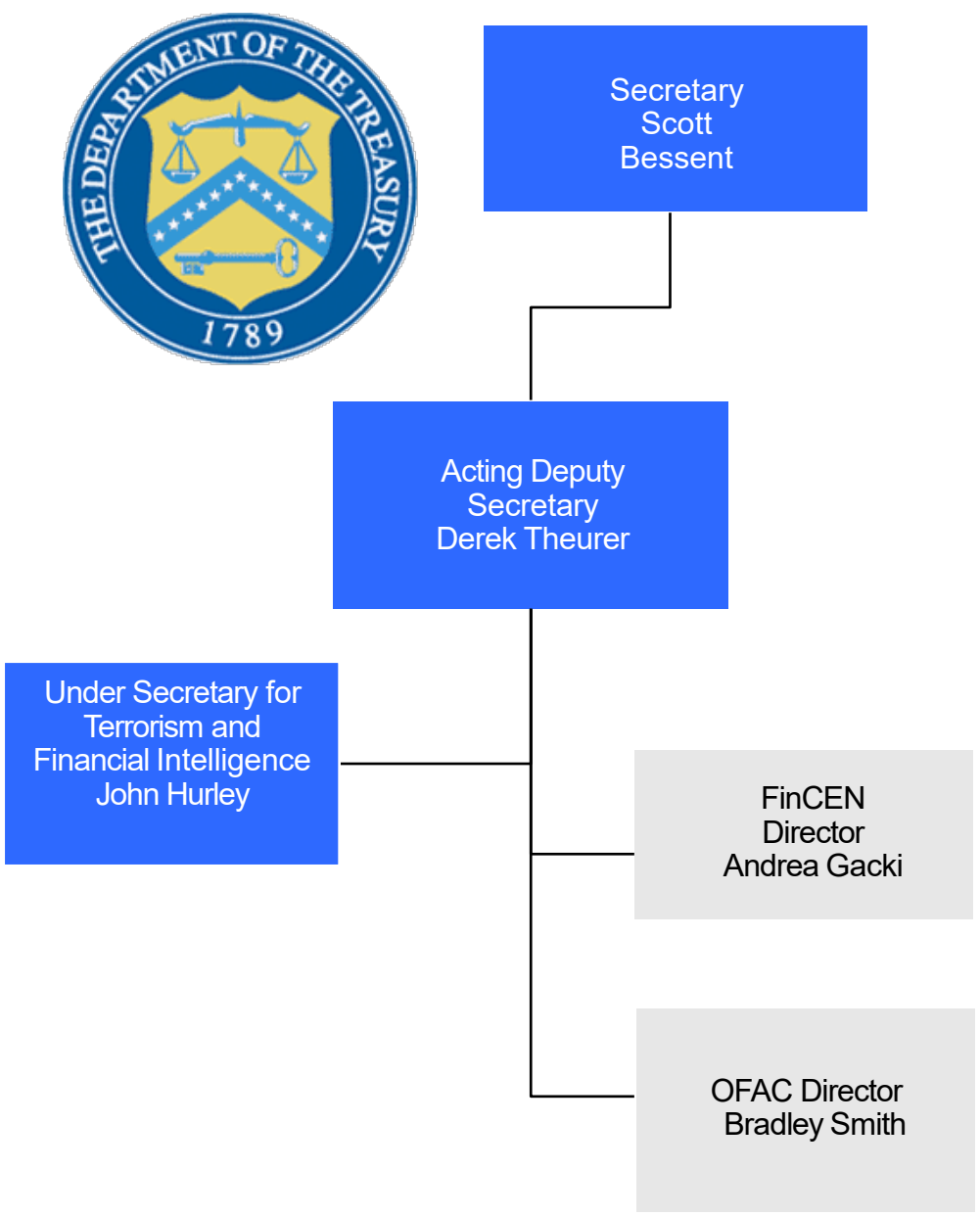
National Security Division

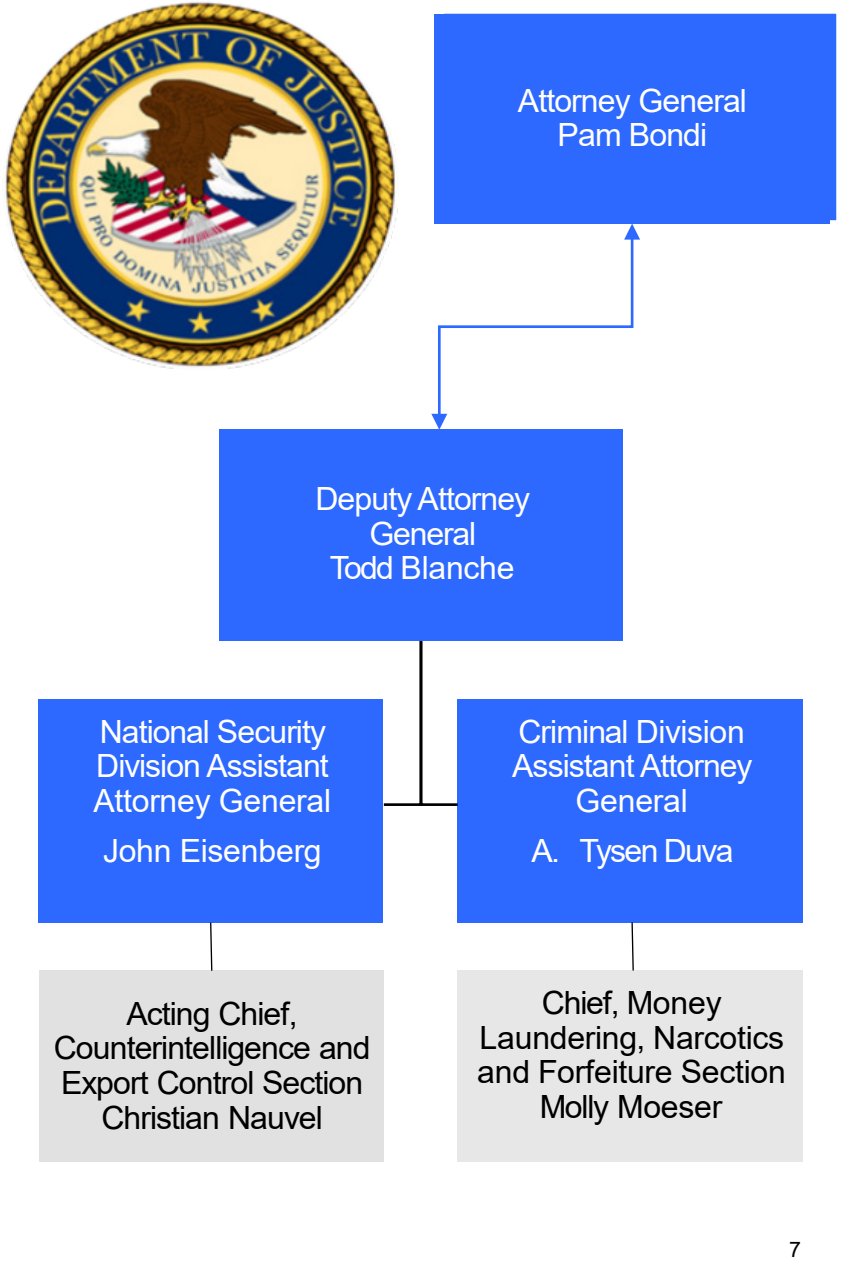
CES

U.S. Attorneys' Offices

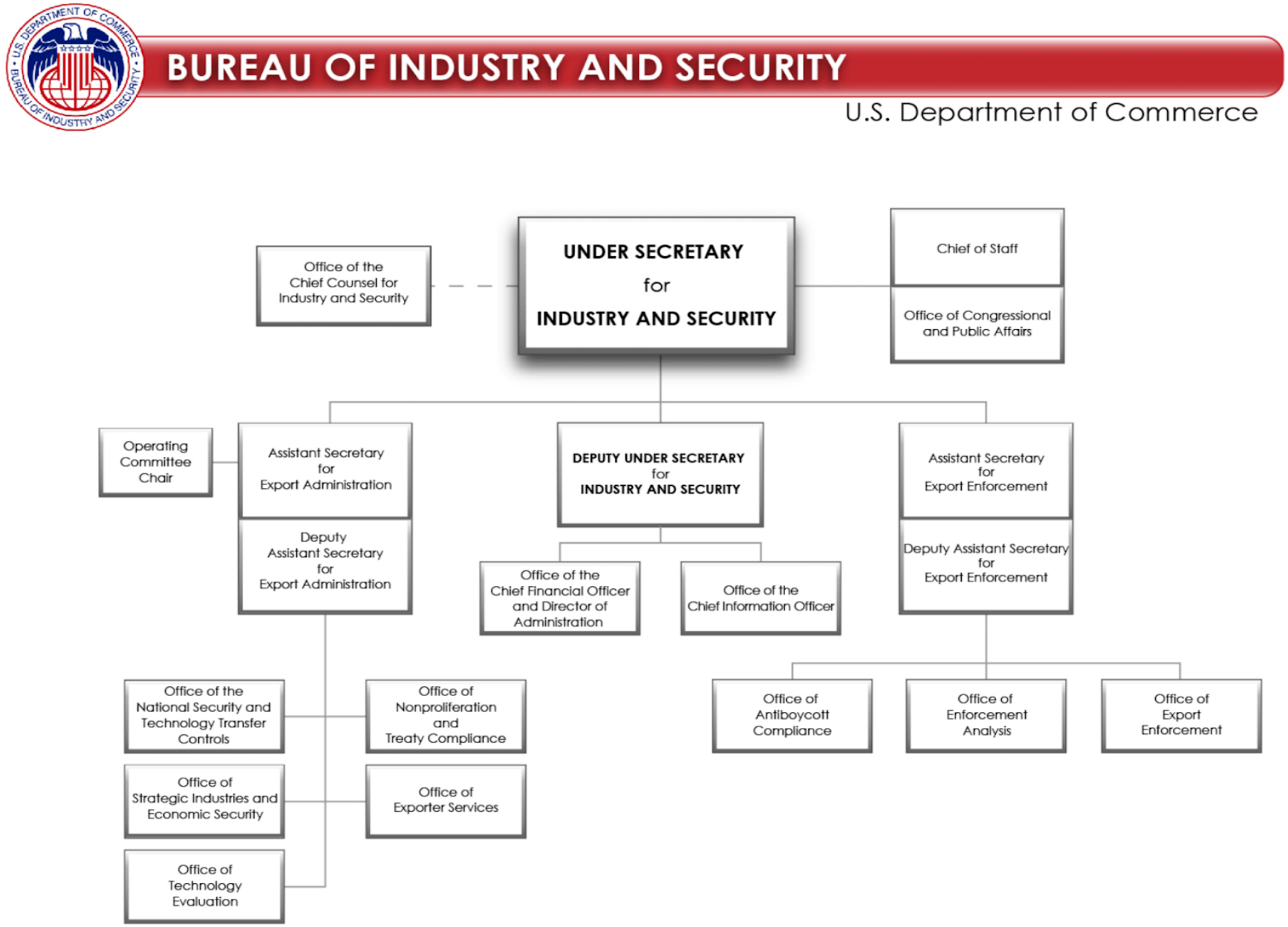
DOJ Civil Division

Treasury and DOJ Key Personnel





BIS Org Chart



Expectations for 2026 and Beyond

02

Expectations for 2026 Across BSA/AML in light of Major 2025 Developments.

1 Continued Active Enforcement with Focus on *Willful Misconduct* and *Underlying Criminal Activity*

- 2025 DOJ guidance reflected a shift towards AML enforcement actions that target willful conduct and underlying criminal activity, and away from regulatory violations.
- DOJ and FinCEN continuing to bring cases consistent with those priorities, particularly in relation to national security and transnational criminal organizations.

2 Federal Regulators *Clarified* Expectations and *Enacted* Regulations Consistent with Priorities

- In 2025, FinCEN and prudential regulators took steps to clarify, tailor, and streamline regulatory requirements and supervisory expectations.
- FinCEN took new regulatory action targeting narcotics trafficking, cross-border remittances, and government benefits fraud.
- We expect similar developments in 2026.

3 State Authorities *Aggressively* Enforced in Light of Perceived Deregulatory Federal Environment

- In 2025, state regulators actively took enforcement actions.
- This was particularly apparent in areas that may be of less federal concern, like financial technology and digital assets companies.

High-ranking officials have continued to emphasize AML Compliance and Enforcement, with further tailoring to reduce regulatory burden.

Scott Bessent Remarks at October 9, 2025 Community Bank Conference

"As part of our broader campaign to modernize illicit finance regulation, FinCEN and the bank regulators are hard at work on a new rule to define the requirements for an effective AML/CFT program. My expectation is that a proposal will recenter supervision where it should be: on the effective effectiveness of a bank's AML/CFT program. I likewise expect that proposal will position FinCEN as a gatekeeper for AML/CFT enforcement."

Andrea Gacki Testimony at September 9, 2025 Hearing Before the House Committee on Financial Services, Subcommittee on National Security, Illicit Finance, and International Financial Institutions

"FinCEN recognizes that there is an urgent need to modernize the AML/CFT regime in the United States so that it is effective, risk-based, and focused on the greatest threats to financial institutions and national security."

FinCEN Press Release on December 22, 2025 Announcing Data-Driven Border Operation to Address Potential Money Laundering

"Failure to comply with the Bank Secrecy Act deprives law enforcement and national security agencies of critical financial intelligence and increases the risk that MSBs can facilitate money laundering and other criminal activity."

John Hurley Remarks at September 17, 2025 Association of Certified Anti-Money Laundering Specialists Assembly Conference

"The best measures of the effectiveness of an AML/CFT program is not how it looks, but first and foremost, how well it captures and proactively reports what law enforcement needs, and secondly, how rarely it fails to identify activity it should be capturing, especially when that activity utilizes known typologies."

Michelle Bowman Testimony at December 2, 2025 Hearing Before the House Committee on Financial Services

"I also support improvements to the Bank Secrecy Act and anti-money-laundering framework that will assist law enforcement while minimizing unnecessary regulatory burden that disproportionately falls on community banks."

Expectations for 2026 Across Sanctions and Export Controls in light of Major 2025 Developments.

1 Continued Active Enforcement with Focus on *Geopolitical Rivals* and *Strategic Technology*

- 2025 civil enforcement actions target financial services and goods provided to Russia, China, and Iran.
- OFAC enforcement against "gatekeepers" representing sanctioned persons through intermediaries.
- Export enforcement actions highlight deceptive practices and compliance program failures.

2 Sanctions and Emergency Powers Used as *Increasingly Unilateral* Foreign Policy Tool Creating Potential for Divergence

- Sanctions targeting ICC, drug cartels, FTOs.
- Tariffs used to address trade imbalances and to negotiate market access apart from traditional institutions.
- Sanctions used in conjunction with military force in Iran, Venezuela.
- Emergency powers on trial at the U.S. Supreme Court.

3 Export Control Policy Shifts as *Personnel and Strategy* are Realigned

- Major rules suspended as Trump Administration pursues different policy goals on AI and U.S.-China trading relationship.
- Personnel shifts signal new approaches and new possibilities.
- Enforcement remains top priority, as BIS receives funding boost for law enforcement activities.

Summary of Major Recent Guidance and Regulatory Action

03

DOJ guidance reflected a shift toward prioritizing AML enforcement actions that target willful misconduct and underlying criminal activity rather than regulatory violations.

- **In April 2025, Deputy Attorney General Todd Blanche issued a memorandum entitled "Ending Regulation by Prosecution," signaling a shift in DOJ enforcement policy in the digital assets space.**
- The memorandum 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 memorandum did not wholly reject enforcement actions for regulatory violations; instead, it stated that such action should only be pursued if the defendant **knowingly and willfully violated a licensing or registration requirement**.

- **On August 21, 2025, Acting Assistant Attorney General Matthew Galeotti further outlined the DOJ's approach in technology-based cases, emphasizing that prosecutors "are not regulators" and will not charge regulatory violations as crimes absent evidence of willfulness.**
- Galeotti noted that "[w]hen bad actors exploit new technologies, it undermines public trust in those technologies and stifles innovation."
- Consistent with the April 2025 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 statements align with the **Criminal Division's White-Collar Enforcement Plan**, which **prioritizes national security threats, complex money laundering, and willful violations that facilitate significant criminal activity**.

FinCEN Clarified Expectations under Existing SAR Regulations to Reduce Compliance Friction

Cross-Border Information Sharing Guidance

- On September 5, 2025, FinCEN issued guidance document regarding confidentiality ("Cross Border Guidance Information Sharing Guidance"), emphasizing 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.”
- 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.

SAR/CTR FAQs

- On October 9, 2025, FinCEN issued FAQs clarifying the expectations related to Suspicious Activity Reports (SAR/CTR FAQs). The SAR/CTR FAQs 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 SAR/CTR FAQs 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.

FinCEN Delayed Implementation of Two Prior Regulations.

Registered Investment Adviser Rule

- Rule previously finalized in September 2024, with effective date of January 1, 2026.
- Rule expands definition of “financial institutions“ required to implement AML program to include Investment Advisers registered (or required to register) with the SEC, and those who report to SEC as exempt reporting advisers.
- On December 31, 2025, FinCEN issued a Final Rule delaying effective date until January 1, 2028.

Real Estate Rule

- Rule previously finalized in August 2024, with effective date of December 1, 2025.
- The rule covers non-financed transfers. A transfer is “non-financed” if it does not involve an extension of credit issued by a financial institution required to maintain an AML program and file SARs. Exemptions for some low-risk types of transfers, e.g. transfers resulting from death, divorce, or to a bankruptcy estate.
- On September 30, 2025, FinCEN issued a Final Rule delaying effective date until March 1, 2026.

Banking Regulators Clarified Regulatory Expectations

Office of the Comptroller of the Currency ("OCC") Guidance for Community Banks

On November 24, 2025, the OCC issued guidance tailoring BSA/AML examination procedures for community banks (institutions with up to $30 billion in assets).

The OCC stated that community banks generally present lower money-laundering and terrorist-financing risks.

Examiners may rely on a bank's actual risk profile, rather than minimum procedural baselines.

The OCC also eliminated community bank reporting through the Money Laundering Risk (MLR) system, removing a longstanding requirement.

Regulators Permitted Greater Flexibility in Customer Identification Practices Under the CIP Rule

On July 31, 2025, the Federal Reserve, OCC, and other federal banking agencies, with FinCEN's concurrence, permitted banks and credit unions to obtain TINs from third parties under the CIP rule.

The change allows institutions to rely on third-party sources, rather than collecting TINs directly from customers.

In an August 5, 2025 supervisory letter, the FDIC clarified that collecting information "from the customer" does not prohibit the use of pre-filled information, provided it is reviewed and submitted by the customer.

The OCC Emphasized Proper Use of SARs in the Context of Debanking

On September 8, 2025, the OCC issued a bulletin previewing potential changes to its BSA/AML supervisory approach as part of efforts to combat debanking.

The OCC reminded banks that customer financial records may be released only in limited circumstances.

Banks "should not use voluntary SARs as a pretext" to disclose customer information or evade the Right to Financial Privacy Act.

Voluntary SARs should be filed only for concrete suspicious activity, even if below reporting thresholds.

President Trump's August 7, 2025 Executive Order "Guaranteeing Fair Banking for All Americans." Combating "Politicized or Unlawful Debanking" has triggered regulatory responses.

Executive Order

- The order defines "Politicized or Unlawful Debanking" ("debanking") as acts by financial services providers to restrict or modify banking products or financial services based on a customer's political or religious beliefs or "lawful business activities that the financial service provider disagrees with or disfavors for political reasons."
- Requires federal banking regulators to remove reputation risk or other concepts that could encourage debanking, and to take action against financial institutions who have engaged in debanking. If the debanking actions were due to a customer's religious beliefs, this can include referring the matter to the Attorney General.
- Requires SBA to give notice to financial institutions for which it guarantees loans to identify and reinstate to debanked parties or offer renewed options for service to parties denied due to debanking actions.

Regulatory Actions

- On September 8, 2025, the OCC announced that it had requested information from 9 largest regulated institutions regarding debanking activities and had reviewed consumer complaint data regarding debanking. It also announced that it considers a "bank's past record and current policies" to avoid debanking when it evaluates factors for licensing activities and CRA ratings.
- On October 7, 2025 the OCC and FDIC issued a joint notice of proposed rulemaking codifying the elimination of reputation risk from their supervisory programs. The proposed rule defines reputation risk and prohibits agencies from taking adverse action against institutions on the basis of reputation risk. It also prohibits agencies from requiring, instructing, or encouraging institutions to close accounts based on specified characteristics perceived as presenting reputation risk. Comments were due for this proposed rulemaking on December 29, 2025.

Treasury Issues

Revised Guidance Regarding the CTA

- The Corporate Transparency Act ("CTA") was enacted in 2021, as part of the 2020 National Defense Authorization Act.
- In 2022, FinCEN adopted a rule to implement the CTA by specifying compliance deadlines and detailing what information must be reported to FinCEN, regarding submission of documentation about beneficial ownership information.
- After months of back-and-forth about the constitutionality of the rule and the CTA in the courts, including in appeals to the Fifth Circuit and Supreme Court, in March 2025, the Department of the Treasury announced and then FinCEN issued an "Interim Final Rule," that removes the requirement for U.S. companies and U.S. persons to report beneficial ownership information to FinCEN under the CTA.
- This Interim Final Rule means that only certain companies, namely those formed under the law of a foreign country and registered to do business in the United States, must file beneficial ownership information with FinCEN, and even then must only disclose information regarding their non-U.S. beneficial owners.
- New York State also rolled out a parallel regulatory regime under state law, which went into effect January 1, 2026.

FinCEN Took *Regulatory Action* Supporting Trump Administration Priorities Related to Combatting Drug Trafficking, Terrorist Financing, and Government Benefits Fraud.

2313a Orders

- On June 25, 2025, FinCEN issued three orders that identified Mexico-based financial institutions as "primary money laundering concern[s] in connection with illicit opioid trafficking."
- These orders are notable as they are the first orders issued by FinCEN pursuant to the Fentanyl Sanctions Act and the FEND Off Fentanyl Act.
- The orders effectively prohibit U.S. financial institutions from engaging in financial transactions with the three entities.
- FinCEN stated that this action reflects an unprecedented commitment by FinCEN to "us[e] all tools at [its] disposal" to target financial institutions that may aid "criminal and terrorist organizations trafficking fentanyl and other narcotics."

Geographic Targeting Orders

- On March 11, 2025, FinCEN issued a Geographic Targeting Order (GTO) "to further combat the illicit activities and money laundering of Mexico-based cartels and other criminal actors along the southwest border of the United States." Pursuant to the GTO and associated guidance, all money services businesses located in 30 zip codes must file Currency Transaction Reports (CTRs) for cash transactions totaling at least $200, effectively reducing the $10,000 threshold that typically applies. This GTO was updated in September 2025. The Order is currently subject to ongoing litigation.
- On January 13, 2026, FinCEN issued a GTO requiring financial institutions in Hennepin and Ramsey counties in Minnesota to retain and report records of certain payments of $3,000 or more, "in furtherance of Treasury's efforts to combat international money laundering of the proceeds of government benefits fraud in Minnesota."

FinCEN Also *Actively Supported* Trump Administration Priorities.

Symposia and Meetings

- Coordinating with foreign financial intelligence units (January 15, 2026);
- FinCEN Exchange focused on denying individual Chinese money launderers access to the U.S. and global financial systems (December 19, 2025);
- Symposium with Canadian FIU (September 15 and 16, 2025);
- FinCEN Exchange focused on combatting narcotics and drug trafficking organizations, at the El Paso Port of Entry (June 27, 2025);
- Public-private partnership event focused on denying Iran access to the global financial system (April 2, 2025).

Guidance Materials

- Alert on cross-border funds transfers involving illegal aliens (November 28, 2025);
- Found transactions with 10 Mexico-based gambling establishments to be of primary money laundering concern (November 13, 2025);
- Identified billions of dollars in Iranian shadow banking activity (October 23, 2025);
- Notice on financially motivated sextortion (September 8, 2025);
- Advisory highlighting Iranian oil smuggling, shadow banking, and weapons procurement typologies (June 6, 2025);
- Alert on oil smuggling schemes on the Southwest Border associated with Mexico-based cartels (May 1, 2025);
- Analysis of fentanyl-related threat patterns and trends in BSA reports (April 9, 2025).

Huione

- **FinCEN findings:** In May 2025, FinCEN identified Cambodian-based **Huione Group** as a **foreign financial institution of primary money laundering concern** under Section 311 of the USA PATRIOT Act.
  - Treasury characterized Huione as a k**ey financial node in Southeast Asia's scam ecosystem**, including networks linked to or adjacent to **Prince Group** operation.
  - FinCEN found that Huione and its subsidiaries processed **at least $4 billion** in **illicit proceeds** between August 2021 and January 2025.
- **Basis for findings:** FinCEN found that Huione operated as a central laundering hub supporting:
  - **North Korea–linked illicit activity**; and
  - Transnational criminal organizations engaged in **cryptocurrency fraud schemes** such as large-scale "pig butchering" across Southeast Asia.
- **Severing access to the U.S. financial system:** In October 2025, FinCEN finalized a rule requiring financial institutions to take steps not to process transactions involving the Huione Group for the correspondent account of a foreign banking institution.
- **OFAC Sanctions:** OFAC simultaneously imposed sanctions designating Huione Group as a TCO and targeting affiliated entities and individuals involved in laundering scam proceeds and facilitating cybercrime.

Federal Reserve, FDIC and OCC Priorities

2025 Federal Reserve Supervision and Regulation Report

Supervisory priorities include (i) credit risk, (ii) liquidity risk, (iii) other financial risk, (iv) other risks, including IT and cyber.

Approximately 2/3 of open supervisory findings in 2025 pertain to governance and controls, which include operational resilience, cybersecurity, and BSA/AML compliance.

FDIC 2025 Annual Performance Plan

Supervisory goals include continuing to perform **risk-based AML/CFT reviews** at each risk management examination.

The FDIC is also focused on continuing to assess the **potential AML/CFT risks of crypto-asset related activities**, and providing supervisory feedback or taking other actions, as appropriate, regarding crypto asset-related activities.

2025 OCC Annual Report

A key area of focus in 2025 remains BSA/AML.

The OCC is also focused on fraud identification, investigations, and suspicious activity report filing processes.

2025 FINRA Regulatory Oversight Report: Anti-Money Laundering, Fraud, & Sanctions

Regulatory Obligations

- FINRA Rule 3310 requires each firm to implement a written AML program reasonably designed to comply with the BSA. Firms must establish AML policies and procedures reasonably expected to detect and report suspicious transactions. AML programs must be independently tested for compliance annually, provide ongoing training for appropriate personnel, and include risk-based procedures for conducting ongoing customer due diligence (CDD).

Investment Fraud Targeting Investors Directly

- FINRA has observed an increase and evolution in investment fraud committed by bad actors who engage directly with investors. Common types of investment fraud include investment club scams, relationship investment scams, imposter websites, and tech support and support center scams.

Findings and Effective Practices

- FINRA found that firms commonly: (a) fail to establish clear policies and procedures concerning Customer Identification Program (CIP) and CDD requirements; (b) inadequately respond to red flags; (c) conduct inadequate CDD; (d) inadequately monitor and report suspicious transactions; and (e) fail to conduct adequate testing of their AML program or provide adequate training for personnel.
- FINRA recommends effective practices, including: (a) investigating unusual withdrawal requests; (b) reviewing clearing firm transactions; (c) reviewing regulatory updates and conducting risk assessments; (d) implementing additional steps for verifying customers' identities for online accounts; (e) delegating AML duties to appropriate business units; and (f) establishing an AML training program.

Continuing Risk: ACH Fraud

- FINRA recently observed an increase in suspicious and fraudulent activity related to ACH fraud, which, according to FinCEN, was the most reported suspicious activity in securities and futures SAR filings between 2014 and 2022. On October 1, 2024, Nacha issued new requirements that all non-consumer participants in the ACH network implement fraud detection and monitoring programs.

Emerging Risk: Adversarial Use of Generative AI

- FINRA has observed that bad actors are increasingly exploiting generative artificial intelligence, amplifying threats to investors, firms, and the securities markets through investment club scams, new account fraud and account takeovers, business email compromise, ransomware attacks, imposter scams, and market manipulation.

2026 SEC Exam Priorities (issued November 2025)

In 2026, the **SEC Division of Examinations** will continue to focus on AML programs and review whether broker-dealers and certain registered investment companies are:

- Appropriately **tailoring their AML program** to their business model and associated AML risks.
- Conducting **independent testing**.
- Establishing an adequate **customer identification program**, including for beneficial owners of legal entity customers.
- Meeting their **SAR filing obligations.**

Registered Investment Companies ("RICs")

- Examinations of RICs will also review policies and procedures for oversight of applicable financial intermediaries.

Registered Investment Advisers (RIAs) / Broker-Dealers

- The Division will review whether broker-dealers and advisers are monitoring the Department of Treasury's Office of Foreign Assets Control sanctions and ensuring compliance with such sanctions.

The Genius Act creates the first comprehensive federal framework governing Payment Stablecoins.

- **Scope:** Signed into law on July 18, 2025, the Act makes it unlawful for any person to issue a payment stablecoin in the U.S. unless the issuer is a **permitted payment stablecoin issuer**.
- **Payment stablecoin definition:** A payment stablecoin is a digital asset intended for use as a payment or settlement mechanism where the issuer:
  - Is obligated to redeem the asset for a fixed amount of monetary value; and
  - Represents, or creates a reasonable expectation, that the asset will maintain a stable value tied to that amount.
- **Permitted Issuers** include federally approved subsidiaries of insured depository institutions and other state or federally qualified entities.
- **Stablecoins issued by non-permitted issuers cannot:**
  - Be treated as cash or cash equivalents for accounting purposes;
  - Be used as margin or collateral by broker-dealers, swap dealers, or other SEC- and CFTC-regulated intermediaries; or
  - Serve as settlement assets for wholesale interbank payments.

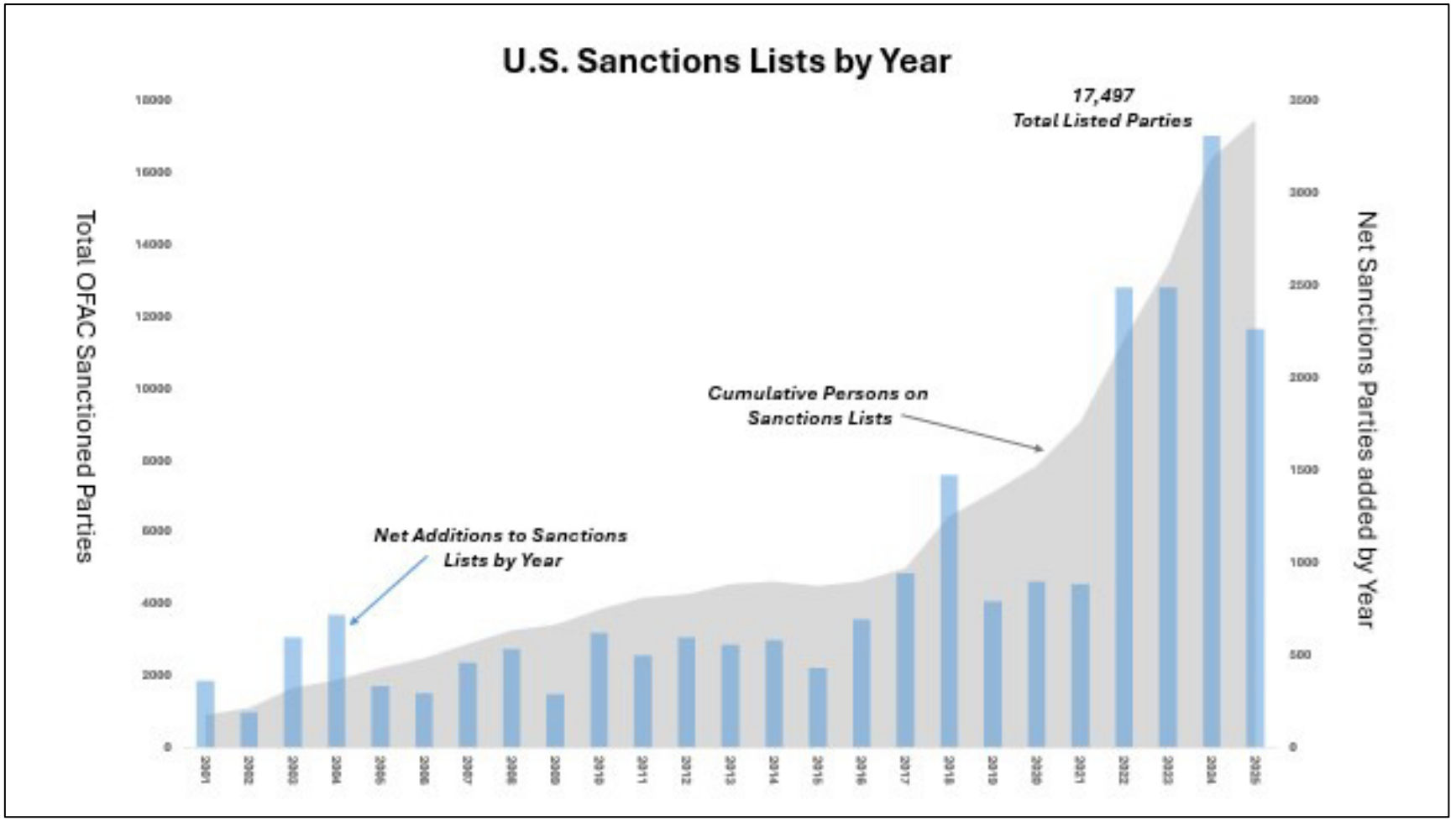
Considerations for AML and Sanctions Compliance

- The Act designates Permitted Issuers as financial institutions under the Bank Secrecy Act, subject to AML, customer due diligence, transaction monitoring, SAR filing requirements with FinCEN, and compliance with OFAC sanctions.
- **Future rulemaking:** Within three years of enactment, FinCEN will issue guidance and rules based on Treasury-led research, risk assessments, and public comments solicited in August and September 2025.
- This guidance will address:
  - Implementation of innovative techniques to detect illicit digital asset activity;
  - Standards for payment stablecoin issuers to identify and report illicit activity, including money laundering, sanctions evasion, and insider trading;
  - Monitoring of blockchain activity, digital asset mixing, and tumbler services; and
  - Risk management standards applicable to financial institutions and decentralized finance protocols.

U.S. Sanctions Developments

04

The number of designations by Treasury, across sanctions programs has evidenced the importance of sanctions as a foreign policy tool, across administrations.



In 2025, **1,764 persons and entities** were added to U.S. sanctions lists resulting in a cumulative total of 17,497 designations.

While this represents a modest pull-back from prior years, it reflects realignment of national security priorities, with Iran and China coming into focus and Russia in an uneasy pause.

Iran Sanctions in 2025: Key Takeaways

Return to "Maximum Pressure" at Scale

- The Trump Administration **fully revived "maximum pressure,"** with the goal to drive Iran's oil exports to zero.
- **OFAC has designated over 900** individuals and entities associated with Iran's activities (the most of any sanctions program last year).
- Heavy focus on **Chinese buyers, shipping networks, and intermediaries**.

Broadening Designations Beyond Oil

- Aggressive OFAC designations against **Iran's shadow banking networks**, including Gulf-based sanctions-evasion hubs.
- Sustained targeting of **defense, missile, UAV, and nuclear procurement networks**, including Iran-Venezuela weapons trade.

Escalation Amid Geopolitical Crisis

- Sanctions intensified alongside **direct U.S. military strikes on Iranian nuclear facilities** during the Israel-Iran conflict in June 2025.
- **Snapback of UN sanctions** triggered new UK and EU measures, deepening Iran's global isolation.
- Renewed **nationwide protests in Iran** over economic collapse and fuel price hikes, met with mixed signals from Washington—including President Trump's public statements suggesting support for Iranian protesters while declining to rule out further U.S. action—leaves uncertainty over whether the U.S. response will center on **additional sanctions (including secondary sanctions and tariffs)** or broader escalation.

Russia sanctions slowed as peace talks evolved.

United States sanctions targeting Russia in 2025 were largely used as a negotiating tool as President Trump attempted to broker a peace agreement between Moscow and Kyiv.

After months without any new sanctions unveiled, the White House announced **secondary tariffs on India**, signaling a **newfound willingness to target certain foreign governments** that import Russian energy, in an attempt to limit the Kremlin's ability to finance its war effort.

As negotiations dragged on, President Trump employed another sanctions tool: the imposition of blocking sanctions on Russia's two largest oil producers—**Rosneft and Lukoil**—carrying **substantial economic consequences**. Aside from these designations, the U.S. targeted **relatively few** Russia-related parties in 2025.

Sanctions targeting Russia in 2026 will depend on whether a Russia-Ukraine deal is reached.

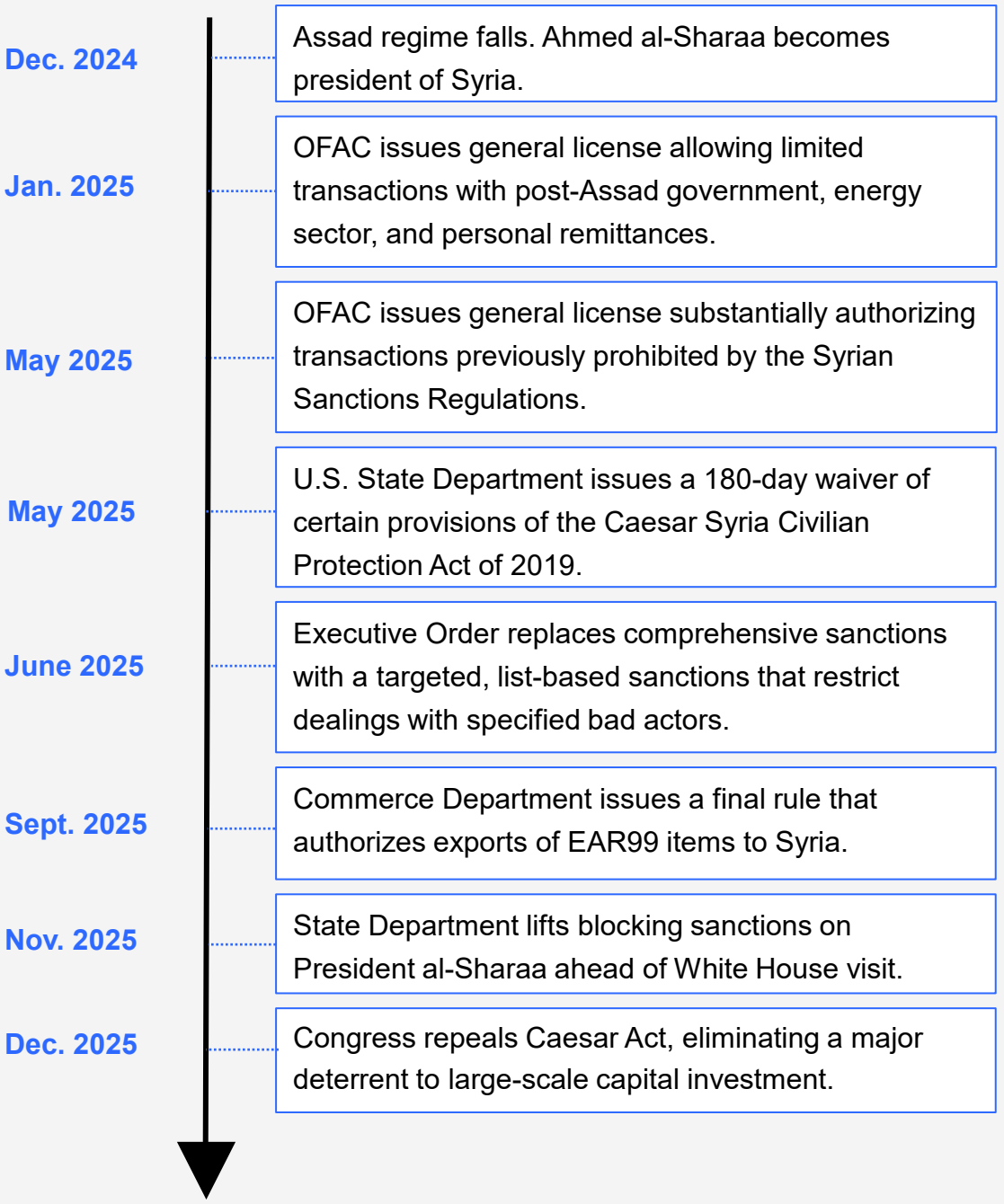
Without an agreement, sanctions could be amplified under pending legislation in Congress (the **Sanctioning Russia Act**) and/or **secondary sanctions** imposed by the White House.

With an agreement, the majority of sanctions restrictions on dealings with Russia could **quickly be relaxed**. Such relaxation, however, could result in a split between the U.S. and its European allies and partners.

Significant sanctions relief for Syria.

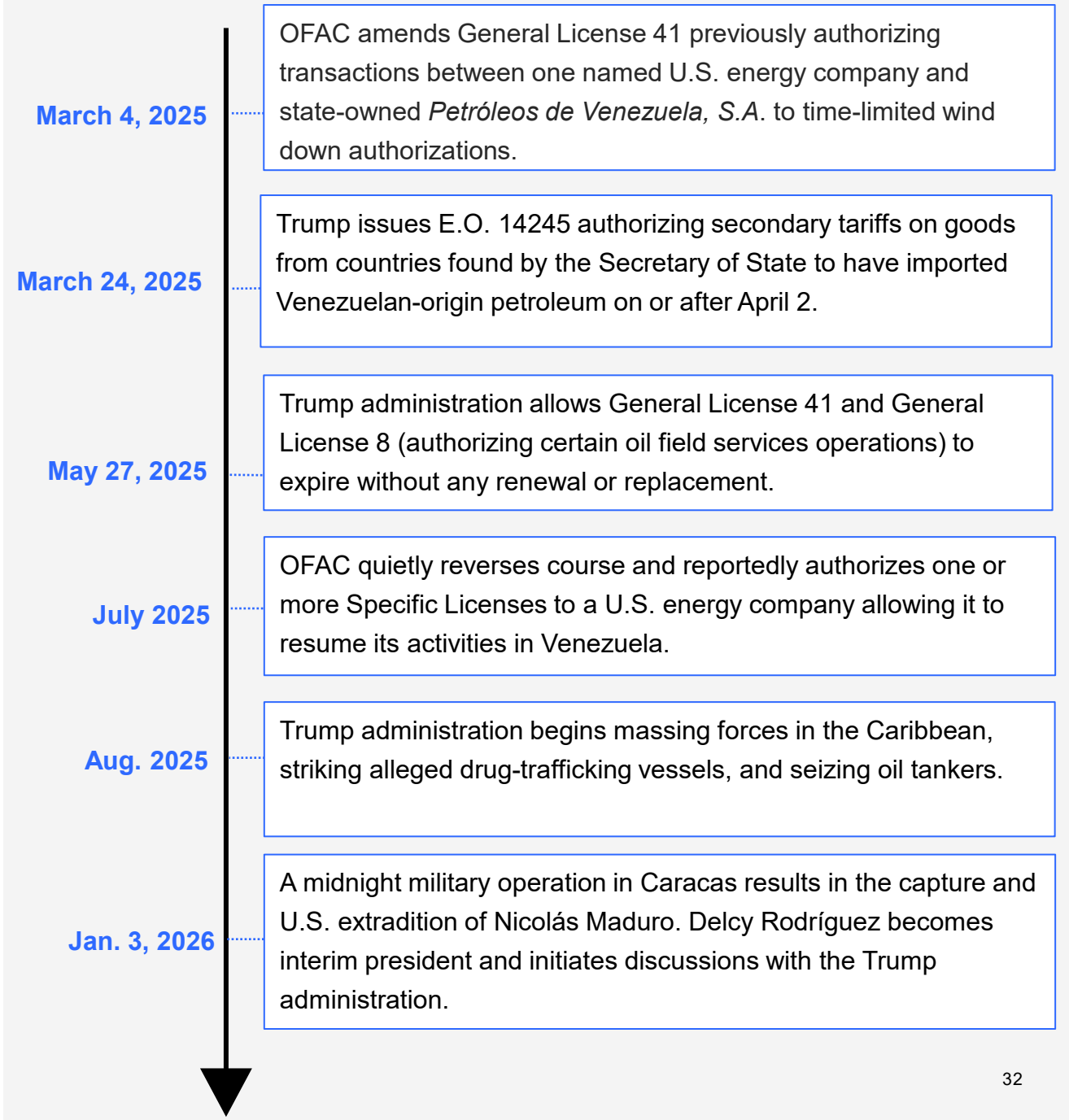
Since the fall of the Assad regime in December 2024, the United States has sought to bolster the government of President Ahmed al-Sharaa, significantly paring back trade restrictions in an effort to help reconstruct the country's economy.

- **Ending of Comprehensive Sanctions**: Following a gradual relaxation of sanctions restrictions in the first half of the year, President Trump issued an executive order revoking the Syrian Sanctions Regulations, which had implemented comprehensive sanctions on Syria's economy. In their place, the administration introduced a list-based sanctions program targeting certain bad actors, including terrorists and supporters of the Assad regime.
- **Easing of Other Restrictions**: Over the course of 2025, the U.S. suspended and then fully revoked secondary sanctions under the Caesar Syria Civilian Protection Act of 2019, lifted blocking sanctions on Syria's president, a formerly designated terrorist, and removed restrictions on exports of goods with civilian uses.
- **Continued Trade Restrictions**: Despite significant sanctions relief, Syria is still home to hundreds of individuals on OFAC's SDN List, remains subject to an arms embargo and restrictions on dual-use goods, and continues to be designated a State Sponsor of Terrorism, restricting U.S. foreign assistance and certain U.S. exports.



The Venezuelan sanctions program remains largely unchanged despite Maduro's arrest.

- In 2025, Trump renewed his first term's hardline stance toward Nicolas Maduro's regime and began "reversing the concessions" given under the Biden administration, including by amending a longstanding general license, permitting that license and another to lapse, and authorizing secondary tariffs on countries importing Venezuelan oil.
- On January 3, 2026, President Trump conducted air strikes across Venezuela's capital, capturing Maduro and bringing him to face drug-trafficking charges in the United States. Following Maduro's arrest, Delcy Rodriguez, the former VP, was sworn in as interim President and immediately established talks with the Trump Administration.
- Currently, U.S. sanctions on Venezuela are not codified by statute and therefore can be quickly modified by executive action. As a first step, the Trump administration has signaled its intent to "selectively roll back sanctions" to permit Venezuelan crude oil to reach global markets.
- On January 9, 2026, President Trump issued Executive Order 14273, prohibiting the attachment or garnishment of Venezuelan oil revenues. On January 29, 2026, OFAC issued GL 46 authorizing many oil-related activities.



The Trump Administration is increasingly deploying counter-terrorism and counter-narcotics sanctions against novel targets.

- **FTO designation of cartels represents a significant shift in the FTO program, where counter-terrorism and counter-narcotics increasingly merge.**
  - During 2025, the U.S. designated a record-breaking **25 entities** as FTOs.
  - The majority of these groups were Mexico-based drug cartels or South American criminal enterprises previously designated under counter-narcotics authorities. **No cartel had previously been FTO-designated.**
  - FTO designation of cartels marks a substantial expansion of the FTO program and suggests that economic sanctions may be used not only as national security tools, but also as levers of immigration and trade policy.
- **FTO designation of cartels increases compliance and trade risks for U.S. individuals and businesses, particularly with business operations in LatAm.**
  - **FTO designation expands criminal liability to those knowingly providing "material support or resources"** to an FTO-designated cartel.
  - This lowered threshold for criminal liability could implicate U.S. business interests in Mexico because of the integration of cartels into certain sectors of the Mexican economy.
  - Material support prosecutions could also target individuals, businesses, or banks in the United States, as well as migrants who engage with purportedly cartel-affiliated smugglers to enter the United States.

FTO and counter-narcotics designations have also increasingly targeted left-wing groups.

- For example, European anti-fascist groups have been designated as FTOs, and the President of Colombia was designated under counter-narcotics authorities.

The Trump Administration created a new ICC sanctions program and has used it to designate ICC-affiliated individuals and entities.

President Trump recreated an unprecedented sanctions program targeting ICC affiliates.

- In a February 2025 Executive Order (E.O. 14203), President Trump created a new sanctions program targeting certain parties associated with the International Criminal Court (ICC).
- Trump previously created an ICC sanctions program during his first term, which was quickly dismantled by President Biden.
- The E.O. describes the ICC as a threat to the sovereignty of states like the U.S. and Israel that are not party to the Rome Statute and have not consented to the ICC's jurisdiction.
- Concurrent with the E.O., the U.S. imposed blocking sanctions against the ICC's chief prosecutor, stemming from his involvement in issuing an arrest warrant against Israeli Prime Minister Benjamin Netanyahu.

15 individuals and entities have been designated under E.O. 14203 thus far.

- 12 individuals and 3 entities have been designated, including ICC prosecutors, ICC judges, the UN Special Rapporteur on the Occupied Palestinian Territories, and NGOs deemed to be supporting ICC investigations of Israeli nationals.
- U.S. persons are restricted from engaging in transactions involving the 15 named parties who appear on the SDN List (as well as those parties' majority-owned entities).
- The ICC itself is not sanctioned; U.S. persons are not generally restricted by OFAC sanctions from engaging in activities involving the ICC or its various organs.

The ICC program shows the Administration's willingness to use sanctions against non-traditional targets.

- Although recent U.S. presidents have consistently maintained the position that the ICC lacks jurisdiction over countries like the U.S. that are not party to the Rome Statute, only President Trump has used sanctions to target the ICC.
- In the future, the Trump Administration could potentially expand existing sanctions to include the ICC itself, particularly if the ICC were to launch an investigation into Trump or other senior U.S. officials.

U.S. Export Control Developments

05

Personnel Changes at BIS

2025 saw massive shifts in personnel at BIS, with the agency undergoing significant turnover.

- A smaller workforce, in combination with the sweeping policy review that took place for much of the year, resulted in **considerable delays** in license application processing.
- The **departure of many career personnel** also created substantial uncertainty surrounding the agency's interpretation of new regulations and policies, how license applications will be assessed, and developments in enforcement action trends.

The primary takeaway from these personnel changes is that exporters cannot take for granted BIS's longstanding construal of the regulations or timely issuance of licenses.

With the increase in BIS's budget, additional hires are expected in 2026.

- Exporters should not expect the personnel shifts in 2025 to decrease the amount of enforcement actions.
- Businesses should keep an eye on trends regarding the **industries and countries involved** in enforcement actions.

Licensing Trends

PRESIDENTIAL ACTIONS

America First Trade Policy

The White House | January 20, 2025

January 20, 2025

MEMORANDUM FOR THE SECRETARY OF STATE

THE SECRETARY OF THE TREASURY

THE SECRETARY OF DEFENSE

THE SECRETARY OF COMMERCE

In early 2025, President Trump instructed BIS to review the entire U.S. export control system, including by identifying and eliminating "loopholes." Results of this review included:

- A regulatory freeze on various Biden-era rules, including a pause on new license applications, which created significant delays and uncertainty across industries;
- Recission of the AI diffusion rule and firearm licensing rule;
- Shutting down the Validated End-User (VEU) program for semiconductor fabs in China, adding a new export-by-export licensing burden on U.S. exporters; and
- Enactment of the Maintaining American Superiority by Improving Export Control Transparency Act, which requires an annual report detailing license applications for certain exports.

The ultimate impact of this review continues to unfold, while BIS has pivoted to issuing shorter rules and amendments.

Rescission of the Biden-Era AI Diffusion Framework & Issuance of New BIS Guidance

- The AI Diffusion Framework (Framework) intended to address loopholes that facilitated Chinese access to restricted chips and compute power to train AI models. The Department of Commerce rescinded the Framework on May 13, 2025. BIS has yet to issue replacement rules.
- On the same day, BIS issued guidance and policy documents signaling a continued tightening of export controls targeting China.
    - Dealing in Chinese advanced ICs, including their purchase or use, without BIS authorization, could create BIS enforcement risks under the EAR's expansive General Prohibition 10.
    - Downstream provision of access to compute power may trigger a license requirement for chip exporters with knowledge that such items will be used to conduct training of AI models for or on behalf of parties headquartered in certain restricted locations and will be used for WMD or military-intelligence purposes.
    - BIS noted transactional and behavioral red flags and suggested due diligence actions for chip exporters to detect and prevent the diversion of advanced computing ICs to China.

"Chip Diplomacy"

- In May 2025, as part of the U.S.-China trade negotiations, the U.S. government permitted the export of advanced GPUs and other equivalent chips to China conditioned on China's continued rare earth shipments. In early January 2026, BIS revised its licensing policy to allow for the export of some of the highest-end GPUs and equivalent chips to China, subject to certain conditions.
- Over the course of 2025, U.S. companies inked multiple deals with the UAE and Saudi Arabia relating to these countries' AI buildout. In furtherance of these initiatives, BIS authorized the export of advanced ICs to certain state-backed AI companies in Saudi Arabia and the United Arab Emirates.

Enforcement Actions against Unlawful Exports of Chips

- In November 2025, BIS announced the arrest and indictment of four individuals who, from September 2023 to November 2025, had illegally transshipped 800 NVIDIA A100 GPUs to China through Malaysia and Thailand.
- In December 2025, BIS announced that it has successfully shut down a sophisticated chip smuggling network that had been illegally exporting advanced GPUs to China and other restricted locations. As alleged, between October 2024 and May 2025, the network knowingly exported or attempted to export at least $160 million worth of export-controlled chips.
- Even with the resumption of the sales of some U.S.-made chips to restricted locations, similar enforcement actions are likely to continue as demands for advanced GPUs remain high.

Overview: The Commerce Department's "Affiliates Rule"

A 50% rule for export-restricted parties – suspended for now

- **Pre-Affiliates Rule**: BIS prohibited end user control took largely "list-based approach." Because the controls targeted only those specifically named in the restricted party lists (Entity List, MEU List), it could be circumvented (e.g., via formation of new subsidiaries).
- **Post-Affiliates Rule:** Shift to "ownership-based approach," similar to OFAC's "50% Rule." Significant expansion of end-user controls. Long-standing "legally-distinct" principle adopted by BIS was abandoned.
  - ***Suspended*** for 1 year (to ~November 9, 2026) in connection with a broader U.S.-China trade deal reached during 2025 APEC Summit.

- **Key aspects**:
  - **Extended export licensing requirements, exceptions, and review policies** to any foreign affiliate owned 50% or more by one or more entities restricted under the (i) BIS Entity List, (ii) MEU List, and (iii) controls targeting certain SDNs under Section 744.8 of the EAR, whether directly or indirectly, individually or in the aggregate.
  - **Imposed the most restrictive license requirements** applicable to one or more of the unlisted affiliates' owners under the EAR.
  - **Imposed heightened due diligence standards** for exporters who have "knowledge" that a foreign party to their transactions has one or more owners that are listed on the Entity List or the MEU List, or that are unlisted entities subject to license requirements or other restrictions based upon their ownership.
  - **Affiliates Rule does not evaluate control and only considers ownership,** though a minority interest by a listed party is an explicit red flag that must be independently resolved before the transaction may proceed.
- *Nexperia* case study: Dutch government seized control of Nexperia, a Dutch-based chip manufacturer owned by Wingtech, a Chinese entity designated on the Entity List. Affiliates Rule would have treated Nexperia as listed on the Entity List as well, cutting it off from U.S. tech.

Sanctions and Export Control Enforcement Actions

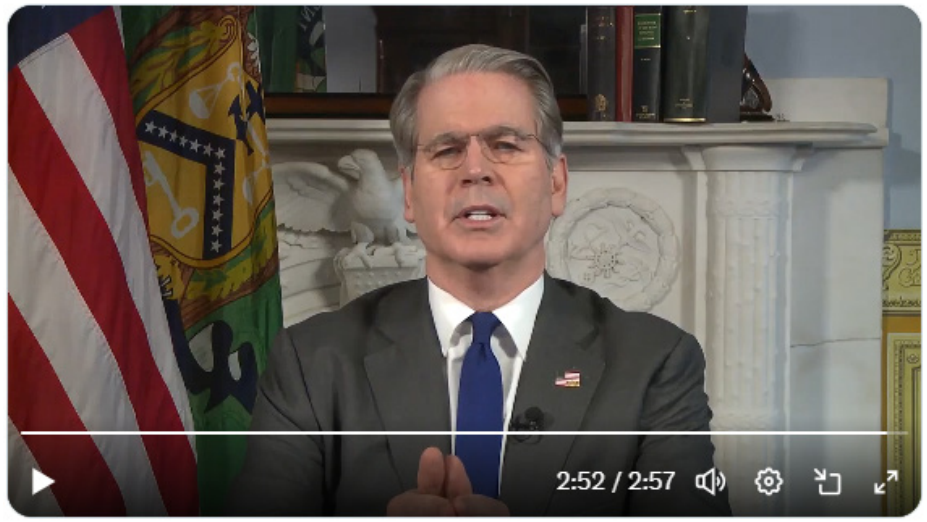
06

Sanctions & export controls enforcers in their own words

Scott Bessent, Secretary of the Treasury

Iran - "*Treasury knows that like rats on a sinking ship, you're frantically wiring funds stolen from Iranian families to banks and financial institutions around the world. Rest assured, we will track them and you. But there's still time if you choose to join us.*"

Cartels - "*The Trump Administration will not allow narcotraffickers to poison Americans… The entire drug trafficking supply chain—from shipping facilitators to money launderers—bears responsibility for American addictions and deaths. We will continue to hold them accountable for the devastation they cause in our homeland.*"



10:33 AM · Jan 15, 2026 · **944.9K** Views

John Hurley, Under Sec. of the Treas. for Terrorism & Fin. Intel.

North Korea - "*North Korean state-sponsored hackers steal and launder money to fund the regime's nuclear weapons program. By generating revenue for Pyongyang's weapons development, these actors directly threaten U.S. and global security. Treasury will continue to pursue the facilitators and enablers behind these schemes to cut off the DPRK's illicit revenue streams.*"

Howard Lutnick, Secretary of Commerce

Enforcement - BIS is on the "intellectual frontline" of an era of "reemerging great power conflict." The new administration will seek "a dramatic increase" in enforcement.

OFAC: Civil Enforcement Overview

In 2025, civil penalties were assessed primarily for committing violations of Russia-related sanctions programs. Iran also remained a significant enforcement target.

Name	Date	Sanctions Program	Sector	Penalties/Settlements Total in USD
Family International Realty LLC and an Individual	January 16, 2025	Ukraine-/Russia-Related Sanctions Regulations (Ukraine/Russia)	Real Estate	$1,076,923.00
Haas Automation, Ltd.	January 17, 2025	Ukraine/Russia	Industrial Equipment	$1,044,781.00
GVA Capital, Ltd.	June 12, 2025	Ukraine/Russia	Investment Management	$215,988,868.00
Unicat Catalyst Technologies, LLC	June 16, 2025	Iranian Transactions and Sanctions Regulations (ITSR), Venezuela Sanctions Regulations (VSR)	Refining Equipment	$3,882,797.00
Key Holding, LLC	July 2, 2025	Cuba Assets Control Regulations (CACR)	Shipping and Logistics	$608,825.00
Harman International Industries, Inc.	July 8, 2025	ITSR, VSR	Audio Equipment	$1,454,145.00
Interactive Brokers LLC	July 15, 2025	ITSR, CACR, VSR, Syrian Sanctions Regulations, Russia Harmful Foreign Activities Sanctions Regulations (RuHSR), Chinese Military-Industrial Complex Sanctions Regulations, Global Magnitsky Sanctions Regulations	Brokerage and Investment Services	$11,832,136.00
Fracht FWO Inc.	September 3, 2025	ITSR, VSR, Weapons of Mass Destruction Proliferators Sanctions Regulations, Global Terrorism Sanctions Regulations	Shipping and Logistics	$1,610,775.00
ShapeShift AG	September 22, 2025	CACR, ITSR, Sudanese Sanctions Regulations	Financial Technology	$750,000.00
An Individual	November 24, 2025	RuHSR	Real Estate	$4,677,552.00
IPI Partners, LLC	December 2, 2025	Ukraine/Russia	Data Center Development	$11,485,352.00
Gracetown, Inc.	December 4, 2025	Ukraine/Russia	Property Management	$7,139,305.00
An Individual	December 9, 2025	Ukraine/Russia	Trust Management	$1,092,000.00
Exodus Movement, Inc.	December 16, 2025	ITSR	Financial Technology	$3,103,360.00
			Total	**$265,746,819**

Gatekeepers and individuals are increasingly targets for OFAC enforcement.

Gatekeepers are at increased risk of facilitating sanctions violations.

- Four OFAC enforcement actions in 2025 targeted "**gatekeepers**" for facilitating blocked persons' access to U.S.-based trust, real estate, and investment assets.
- Gatekeepers, including investment advisors, accountants, attorneys, trust and corporate formation services providers, and real estate professionals, occupy positions of trust and lend an air of legitimacy to transactions with sanctioned parties.
- Gatekeepers may be subject to heightened due diligence expectations and should carefully screen prospective clients.

Enforcement risk is not limited to corporate entities.

- Three unnamed **individuals** were subject to substantial penalties for providing professional services to blocked persons.
- The increasing focus on individual liability is a departure from OFAC's recent practice of levying fines primarily against corporate entities.
- Gatekeepers and individuals should familiarize themselves with their sanctions compliance obligations and common red flags for blocked persons—including when blocked persons are involved in transactions through proxies or opaque legal structures.

"[G]atekeepers should remain vigilant of the risk that unscrupulous actors, including sanctioned persons or their proxies, may seek to use professional services to conceal a property interest or otherwise evade OFAC Sanctions."

U.S. persons face substantial risks "when relying on formalistic ownership arrangements that obscure the true parties in interest behind an entity or investment, without sufficiently considering factors such as a control or influence over that investment."

Disregard of OFAC notices and outreach leads to substantial penalties.

GVA Capital, Ltd.: Gatekeepers cannot rely on formalistic ownership arrangements.

- U.S.-based investment fund solicited and managed blocked Russian oligarch's U.S. investments.
- Fund managers relied on formalistic ownership arrangements that concealed blocked person's involvement on paper, but knew the true origin of the funds.
- GVA Capital continued to manage the blocked funds after receiving an OFAC blocking notice and administrative subpoena.

An Individual (Nov. 2025): Resale of blocked property at public auction leads to hefty penalties.

- Individual acquired blocked residential property at public auction; subsequently mortgaged, refurbished, and sold the property to unwitting third party.
- Individual disregarded OFAC blocking notice and certified (falsely) that they had complied with the cease-and-desist.
- OFAC noted that buyers of blocked property can incur liability even when blocked party's name does not appear on relevant deeds or transactional documents.

OFAC may be less willing to settle where it intends to convey a message.

- Vast majority of OFAC enforcement actions resulting in monetary penalties are resolved with settlement agreements.
- Issuance of penalty notices—*i.e.*, non-negotiated penalties imposed by OFAC—are rare and often litigated against by enforcement targets.
- OFAC's imposition of three penalty notices in 2025 for egregious violations of sanctions involving blocked Russian oligarchs signals OFAC's seriousness about deliberate violations and its willingness to litigate if necessary.

DOJ increases focus on sanctions evasion.

White Collar Enforcement Plan positions sanctions evasion as criminal and national security concern.

- DOJ's Criminal Division is directing its focus on gatekeepers, financial institutions, and others who facilitate sanctions evasion by drug cartels, transnational criminal organizations, hostile nation-states, and foreign terrorist organizations.
- Although business-friendly "America First" enforcement approach could lead to fewer or less aggressive prosecutions, U.S. Attorney's offices are increasingly empowered to pursue prosecutions against financial institutions facilitating sanctions evasion.

North Korean IT Worker Scheme: Aggressive action in 2025 to disrupt DPRK sanctions evasion efforts.

- Multi-agency push in 2025 to prosecute and sanction parties involved in North Korean efforts to generate hard currency by fraudulently placing DPRK IT workers in hundreds of U.S. companies.
- Actions included seizure of 29 financial accounts, five guilty pleas, and over $15 million in civil forfeiture actions, plus OFAC designation of non-U.S. parties implicated in scheme.
- We expect DPRK sanctions evasions efforts to continue in 2026, including by positioning IT workers in U.S. tech companies to draw salaries and exfiltrate sensitive or export-controlled data.

BIS Corporate Enforcement Actions Since January 2025

Since 2025, corporate enforcement actions were brought primarily for committing export control violations related to Russia, China, and Iran. Despite significant personnel changes, enforcement did not slow.

Names	Date	Charges	Sector	Outcome
Eleview International Inc.	October 23, 2025	Unlicensed export of controlled items to Russia	Shipping and Logistics	$125,000.00 in civil penalty
Luminultra Technology, Inc.	September 30, 2025	Unlicensed export of luminometers and aqueous test kits to Iran	Industrial Equipment	$685,051.00 in civil penalty
Hallewell Ventures, Ltd.	September 30, 2025	Unlicensed reexport of aircraft to Russia	Aviation	$374,474.00 in civil penalty
Andritz Inc.	July 29, 2025	Unlicensed export of refiner plates to Russia	Industrial Equipment	$1,577,397.18 in civil penalty
Cadence Design Systems, Inc.	July 28, 2025	Unlicensed export of EDA and chip design technology to China	Technology	$95,312,000.00 in civil penalty
Alpha and Omega Semiconductor Incorporated	June 27, 2025	Unlicensed export of smart power stages, controllers, and related accessories to China	Technology	$4,250,000.00 in civil penalty
Haas Automation, Inc.	January 17, 2025	Unlicensed export of machine parts to Russia and China	Industrial Equipment	$1,500,000.00 in civil penalty
			Total civil penalties	**$103,823,922**

The Department of Justice announced two declinations over company violations of national security laws, including export control laws.

Both declination decisions were made pursuant to the DOJ NSD's **Enforcement Policy for Business Organizations**, with the latter case comprising the first ever application of its **Voluntary Self-Disclosures in Connection with Acquisitions Policy**. These examples show that companies, upon discovering misconduct, can benefit from taking actions such as making a timely **voluntary self-disclosure** ("VSD"), proactively **cooperating** with DOJ, and undertaking prompt and effective **remediation**.

Universities Space Research Association

- An employee of the firm willfully provided flight control software to a prohibited Chinese entity.
- When it discovered the misconduct as part of an internal investigation, the firm disclosed it to DOJ NSD in a timely and voluntary manner.
- The DOJ issued its declination in April 2025, citing a number of mitigating factors.
- In addition to a VSD, the company was credited with providing exceptional and proactive cooperation to the government and undertaking timely and appropriate remediation, among other considerations.
- The employee was indicted, pleaded guilty, and was sentenced to 20 months' imprisonment.

White Deer Management, LLC/Unicat Catalyst Technologies, LLC

- White Deer acquired Unicat and within a year discovered a number of Unicat chemical catalyst sales to customers in Iran, Syria, Venezuela, and Cuba by target company's CEO.
- White Deer made a timely-under-the-circumstances VSD of its discovery to NSD, provided exceptional and proactive cooperation to its investigation, and swiftly redressed misconduct.
- DOJ issued its declination in June 2025, noting that it was despite the presence of aggravating factors (including involvement in the violations by senior management).
- Unicat entered into a non-prosecution agreement, receiving credit for White Deer's VSD.

Recently Announced Enforcement Actions in 2026

Exyte Management GmbH

- Stuttgart-based corporate group.
- Subsidiary in Shanghai procured over $2.8 million worth of goods from suppliers in China for SMIC Beijing, a party on the Entity List.
- Group corporate compliance program failed to adequately address the application of the EAR to **in-country transfers outside of the United States**.
- Company self-disclosed.
- Civil penalty imposed of $1.5 million.

Names	Charges	Outcome
Individual (Dual U.S.-Russian citizen) **Jan 15, 2026**	Attempted to illegally export aircraft from the U.S. to Russia through Armenia	41 months in federal prison with three years of supervised release
Individual (Indian citizen) **Jan. 16, 2026**	Conspired to export controlled aviation components and system to Russia	30 months in federal prison
Individual (Japanese citizen) **Jan 22, 2026**	Illegally exported 900 firearms components and accessories, including AR-15 lower receiver parts kits, upper receivers, magazines, and similar components with the intent to use those items for airsoft purposes	Pled guilty; faces a maximum term of imprisonment of 20 years, a fine of up to $1,000,000 and a period of supervised release of up to three years

BSA/AML Enforcement Actions

07

ENFORCEMENT TREND
ALLEGED WILLFUL MISCONDUCT FACILITATING CRIMINAL ACTIVITY

Former President of Oklahoma Bank

- In December 2025, DOJ announced the **indictment and arrest** of the former President and Chief Executive Officer of First National Bank of Lindsay for **failure to implement an adequate AML program**, among other charges, in the U.S. District Court for the Western District of Oklahoma.

- The defendant also served, at various times between February 2007 and September 2024, as the bank's **Chief Financial Officer, IT Officer, BSA Officer, and Compliance Officer**.

- **DOJ alleges** that the defendant:
  - Caused the bank to issue **loans that were never repaid**;
  - **Manipulated bank records** to overstate loan performance;
  - **Provided false records** to the OCC and the bank's Board of Directors;
  - **Failed to file SARs** related to his own alleged fraudulent scheme; and
  - **Advised customers to structure cash deposits below $10,000** to evade reporting requirements.

- **Willful Misconduct:** DOJ stated that the charges reflect the Administration's priorities because the conduct was **willful**—the defendant allegedly knew his BSA obligations—and because the AML failures **facilitated and concealed underlying criminal activity**.

ENFORCEMENT TREND
REDIRECTED DIGITAL ASSET ENFORCEMENT

Paxful

- On December 9, 2025, **Paxful** pleaded guilty to conspiring to violate the BSA and to operate an unlicensed money transmitting business under 18 U.S.C. § 1960.
- **DOJ alleged the platform** was used to facilitate money laundering, sanctions violations, and other crimes, including fraud, romance scams, extortion, and commercial sex-related offenses.
  - Marketed itself as not requiring KYC;
  - Allowed customer use without collecting required KYC;
  - Provided fake AML policies to third parties; and
  - Failed to file required SARs.
- **Outcome:** The platform agreed to pay a $4 million fine.
  - Reduced from an agreed-upon $112.5 million fine due to inability to pay;
  - The agreed-upon fine reflected a 25% cooperation reduction from the bottom of the Sentencing Guidelines range.
- **Parallel action:** FinCEN imposed a $3.5 million civil penalty for MSB registration, AML, and SAR violations, crediting $1.75 million of the DOJ criminal penalty toward the civil resolution.
- **Past enforcement against the platform:** In 2024, the platform's co-founder/CTO pleaded guilty to AML conspiracy charges, agreed to pay a $5 million fine, resigned, and agreed not to serve in future management at the platform.

Co-founders of Samourai Wallet

- In November 2025, Judge Denise Cote (S.D.N.Y.) sentenced the co-founders of Samourai Wallet **to four- and five-year prison terms** following their July 2025 guilty pleas to conspiracy to operate an unlicensed money transmitting business.
- **Samourai Wallet** operated as a cryptocurrency service that facilitated non-traceable private transactions designed to obscure transaction provenance.
- **Alleged Crime:** Samourai allegedly processed billions of dollars in transactions and was used to launder criminal proceeds, including activity tied to sanctions evasion and other illicit conduct.
    - **Knowledge and Intent Element:** The government asserted that the co-founders **knowingly** continued to operate and profit from the platform despite awareness that users relied on Samourai's services to evade law enforcement detection.
- **Charges:** The original indictment, unsealed in April 2024, charged conspiracy to violate:
    - 18 U.S.C. § 1960(b)(1)(B) (operating without required FinCEN registration);
    - and § 1960(b)(1)(C) (knowing transmission of criminal proceeds or funds intended to promote unlawful activity.
- **Post-Memo Adjustment:** Following DOJ's April 2025 "Ending Regulation by Prosecution" memorandum, prosecutors filed a superseding indictment omitting the § 1960(b)(1)(B) registration-based allegation.
- **Sentencing Emphasis:** In its sentencing submissions, DOJ focused on allegations that the co-founders repeatedly solicited and encouraged criminal actors to use Samourai Wallet to conceal transfers of criminal proceeds.

Tornado Cash Verdict

- **Tornado Cash:** an open-source crypto anonymity protocol that DOJ alleged was used to anonymize more than $1 billion in illicit proceeds.

- **Trial:** In July 2025, Roman Storm proceeded to trial in SDNY for his role in creating and maintaining Tornado Cash. The indictment charged Storm with conspiracy to:
  - Commit money laundering;
  - Violate U.S. sanctions;
  - Operate an unlicensed money-transmitting business initially under 18 U.S.C. § 1960 (b)(1)(B) and § 1960(b)(1)(C), but amended to only § 1960(b)(1)(C) following DOJ's April 2025 *Ending Regulation by Prosecution* memorandum.

- **Mixed Verdict:** After a four-week trial, the jury returned a mixed verdict on August 6, 2025, convicting Storm of conspiracy to operate an unlicensed money-transmitting business, but failing to reach a verdict on the money laundering and sanctions charges, resulting in a mistrial on those counts.

Evita

- On June 9, 2025, DOJ charged Iurii Gugnin, the founder, President, Treasurer and Compliance Officer of U.S.-based Evita Investments Inc. and Evita Pay Inc. with charges including money laundering, operating an unlicensed money transmitting business, and violating the BSA, among other charges.

- DOJ alleged Gugnin used his cryptocurrency company Evita to funnel more than $500 million of overseas payments through U.S. banks and cryptocurrency exchanges while hiding the source and purpose of the transactions. Evita allegedly served as a means to launder hundreds of millions of dollars for sanctioned Russian entities and obtain export-controlled technology for the Russian government.

- Charges are currently pending.

- Charges sit at the intersection of different Administration priorities.

ENFORCEMENT TREND
COORDINATED ACTION WHERE PRIORITIES COMBINE

Prince Group: Coordinated Criminal, Civil, and Sanctions Actions

- **Coordinated enforcement action:** 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 operated as a **transnational criminal organization** built around forced-labor scam compounds, where trafficked individuals were compelled to run "pig butchering" **cryptocurrency investment fraud schemes** targeting victims worldwide.
- **Criminal indictment:** DOJ unsealed a criminal indictment in the Eastern District of New York charging alleged **Prince Group chairman Chen Zhi** describing:
  - the Prince Group's public-facing real estate, banking, and hospitality businesses masked a sophisticated criminal infrastructure that generated billions in victim losses; and
  - that a Prince Group-linked network operating in Brooklyn **laundered more than $18 million in victim funds** through New York shell companies between 2021 and 2022.
- **Civil complaint:** DOJ also unsealed a civil forfeiture complaint seeking approximately **127,271 Bitcoin**—valued at roughly $15 billion at the time of seizure—allegedly constituting proceeds and instrumentalities of Prince Group's wire fraud and money laundering schemes.
  - The complaint alleges laundering techniques including commingling illicit proceeds with newly mined cryptocurrency, complex wallet layering, and repeated "spraying" and "funneling" transactions designed to obscure the source of funds.
- **OFAC sanctions:** In a parallel action, OFAC designated Prince Group as a Transnational Criminal Organization and **imposed sanctions on 146 associated targets**, including Chen Zhi, senior executives, and affiliated companies across the group's global corporate network.

FinCEN Enforcement Operation Targeting MSBs Along Southwestern Border

On December 22, 2025 FinCEN announced an operation targeting more than **100 MSBs operating along the southwest border**, based on a review of over one million CTRs and 87,000 SARs.

- FinCEN is examining these MSBs for “potential non-compliance with regulations designed to detect money laundering and combat illicit finance.”
- The Treasury Department reports that this is a "**first-of-its-kind, data-driven enforcement operation**" that will apply "**high-performance data processing** to uncover illicit networks and protect the U.S. financial system."

FinCEN is coordinating with the **Homeland Security Task Force, IRS, and state and federal regulators and law enforcement.**

- Thus far, the operation has resulted in six notices of investigation, “dozens” of examination referrals to the IRS, and over 50 compliance outreach letters.
- Based on its findings, FinCEN will impose civil money penalties, pursue civil injunctive actions, issue warning letters, and make referrals to criminal authorities for willful BSA violations.

The Treasury Department stated that this operation is consistent with the Trump Administration's **"directive to secure the border"** and that the Department is “utilizing all tools to stop terrorist cartels, drug traffickers, and human smugglers.”

ENFORCEMENT TREND
GOVERNANCE STRUCTURE FOCUS

FDIC Enforcement Actions

The Federal Deposit Insurance Corporation (FDIC) remains active in 2025, highlighting deficiencies in Governance Structure.

- On April 3, 2025, **Hatch Bank** entered a Consent Order with the FDIC for alleged violations of the BSA and FDIC regulations and deficiencies in its AML/CFT Program. The Consent Order requires the board to implement effective risk assessments, independent testing, and internal controls addressing program resources, third-party relationships, AML/CFT monitoring and reporting standards, and customer due diligence.

- On May 15, 2025, **Quaint Oak Bank** entered a Consent Order with the FDIC for alleged violations of the BSA and FDIC regulations and unsafe and unsound banking practices relating to its AML/CFT Program. The consent agreement requires increased board oversight of the bank's AML/CFT program and the adoption of a third-party risk management program, a AML/CFT program, a sufficient OFAC compliance program, and a board of directors compliance committee to monitor the progress of each program. The bank is also required to furnish FDIC with quarterly progress reports.

- On August 15, 2025, **Unity Bank of Mississippi** entered a Consent Order with the FDIC for alleged BSA violations. The Consent Order Action requires the bank to present a plan detailing actions they will take to correct AML/CFT program deficiencies and create a board oversight committee receiving monthly reports detailing the progress of the order. Among other actions, the bank must also revise its AML/CFT Program, perform an annual ML/TF risk assessment and independent AML/CFT program testing, and implement internal controls concerning customer due diligence, SARs, and CTRs.

OCC Enforcement Action

On October 16, 2025, the OCC announced a formal agreement with First National Bank of Pasco to address unsafe or unsound practices that included deficiencies in BSA/AML risk management and suspicious activity reporting.

- This enforcement action is representative of the OCC's general focus on **governance structures** addressing BSA/AML risk and heightened expectations relating to **Board oversight and involvement**.

Under the agreement, the bank committed to:

1. Appoint an **AML Officer** with independence, authority and resources, and reports to the board and senior management.
2. Adopt **AML/BSA policies and procedures**, that include risk-based transaction limits, sufficient information management systems, and procedures for customer due diligence, transaction investigations, and SAR and CTR filing.
3. Establish a **Customer Due Diligence program** that creates risk-rating categories, outlines methodologies and procedures classifying customers, and procedures for periodic reviews and monitoring of those categories.
4. Establish a **Suspicious Activity Reporting program** that sets procedures for dispositioning, evaluating, and timely reporting suspicious activity and promptly communicates backlogs to the Board and management for resolution.
5. Adopt an **independent testing program** that evaluates the Bank's BSA/AML compliance and promptly reports deficiencies to the Board or BSA/AML Audit Committee.
6. Establish a **compliance committee** to receive quarterly progress reports.

First National Bank of Pasco
ESTD 1986

State Enforcement Actions

In April, July, and August 2025, state regulators including in New York, Massachusetts, Texas, California, Minnesota, and Nebraska reached resolutions with financial technology companies for alleged AML deficiencies.

- Those alleged deficiencies included:
  - Inadequate customer due diligence;
  - Inadequate AML program oversight;
  - Deficient monitoring and reporting of suspicious activity;
  - Data integrity and transaction monitoring issues;
  - Failure to timely remediate prior compliance issues;
  - Transaction alert backlog, and
  - Violation of remittance rules.

ENFORCEMENT TREND
CRYPTO KIOSKS

California Enforcement Action Against Multiple Crypto Kiosks

2025 marked the California Department of Financial Protection and Innovation's (DFPI) first year of enforcement under Digital Financial Assets Law (DFAL), which was enacted in 2023.

- **Crypto Kiosk Enforcement Actions:** In 2025, DFPI announced enforcement actions against multiple crypto kiosk operators for alleged violations of the DFAL.

- **Significant action:** DFPI noted as an example of an operator that, since January 2024, had:
  - Charged fees and markups exceeding DFAL's statutory limits;
  - Accepted cash transactions above DFAL's $1,000 daily cap; and
  - Failed to provide required pre-transaction disclosures and complete transaction receipts.
- The operator was ordered to pay $675,000, including $105,000 in consumer restitution.

- **Broader enforcement activity:** 2025 also saw other DFAL fines and multiple desist-and-refrain orders against other crypto kiosk operators.

DFPI
DEPARTMENT OF FINANCIAL PROTECTION & INNOVATION

FinCEN Issued Notice on Crypto Kiosks

In August 2025, FinCEN issued a notice urging financial institutions to be vigilant in identifying and reporting suspicious activity involving crypto kiosks.

- **Identify that** crypto kiosks can be exploited by illicit actors including scammers.
- Risk is **exacerbated** if kiosk operators fail to meet their BSA obligations.
- Illicit activity involving crypto kiosks includes **fraud**, certain types of **cybercrime**, and **drug trafficking organization** activity, which are three national priorities.
- Highlights the rise in **scam payments** facilitated by crypto kiosks.
- Recognize disproportionate effect on **older adults**.

ENFORCEMENT TREND
ACTIVE FINRA ENFORCEMENT

The Financial Industry Regulatory Authority (FINRA) remains active in the AML/BSA space, with enforcement actions clustering around several recurring themes:

1 *Failure to conduct required annual independent AML testing*

- Expect regulators to continue bringing enforcement actions based on **technical and procedural failures**, including the absence of required independent AML testing, even where there is limited evidence of underlying suspicious activity.

2 *Deficient AML supervisory systems and SAR monitoring*

- Heightened enforcement focus on whether firms' AML systems are **reasonably designed to identify, escalate, and report suspicious activity**, with particular scrutiny of firms that fail to tailor monitoring and red flags to their business model or that miss SARs at scale.

3 *AML Officer / CCO accountability and governance failures*

- Regulators increasingly emphasize **compliance governance and individual accountability**, including actions against CCOs and AML Officers where failures in oversight, escalation, or response to red flags reflect structural weaknesses rather than isolated errors.

Deficiencies in AML Programs and Independent Testing

The Financial Industry Regulatory Authority (FINRA) remains active in 2025, highlighting alleged deficiencies in AML Programs and Independent Testing.

- **A Swiss private bank** was fined $650,000 for its alleged inadequate AML program. Allegations included 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.

- **An investment banking and wealth management firm** was fined $30,000 for allegedly failing to conduct independent testing of its AML program for 13 years.

- **A broker-dealer** was fined approximately $1.1 million in July 2025 for alleged supervisory and AML program deficiencies. Allegations included failing to conduct required independent testing of its AML program and failing to establish and implement reasonably designed AML policies, procedures, and training, along with broader supervisory failures related to short-selling activity and compliance oversight.

- **A broker-dealer** was censured and fined $475,000 in March 2025 for alleged AML and supervisory deficiencies. FINRA alleged that the firm's AML program was not reasonably designed to detect and report suspicious activity, including potentially manipulative trading, and that the firm failed to conduct reasonable independent testing of its AML program over multiple years.

Deficiencies in AML Programs and Independent Testing

The Financial Industry Regulatory Authority (FINRA) remains active in 2025, highlighting deficiencies in AML Programs and Independent Testing.

- **A broker-dealer** was fined $20,000 in July 2025 for alleged net capital, books and records, and AML violations. Allegations included failing to maintain accurate net capital computations and FOCUS filings over an extended period, failing to timely notify regulators of a net capital deficiency, and failing to conduct an annual independent test of its AML compliance program.

- **A broker-dealer** was fined $55,000 in April 2025 for alleged Reg BI, net capital, books and records, and AML violations. Allegations included failing to conduct independent testing of its AML program and failing to maintain written AML policies addressing the testing requirement, as well as supervisory failures related to recommendations of non-traditional exchange-traded products and inaccurate net capital and FOCUS reporting.

- **A broker-dealer** was censured and fined $15,000 in February 2025 and required to certify that it conducted an independent test and revised its AML program. FINRA alleged that the firm failed to conduct any independent testing of its AML program for multiple years and failed to maintain written AML procedures requiring annual independent testing.

SAR Monitoring and Reporting Programs

FINRA Enforcement in 2025 also Highlighted Weaknesses in SAR Monitoring and Reporting Programs

- **A broker-dealer** was fined $400,000 for alleged AML program deficiencies related to SAR monitoring and reporting. FINRA alleged that the firm failed to reasonably monitor and investigate suspicious transactions, including outgoing wire transfers, and failed to properly review and escalate alerts generated by its third-party transaction monitoring system.

- **A broker-dealer** was fined $100,000 for AML deficiencies tied to SAR monitoring and reporting following the launch of a new business line. FINRA alleged that the firm onboarded hundreds of customers in high-risk foreign jurisdictions but relied on manual blotter reviews without effective exception reports or automation, failing to reasonably identify and investigate suspicious activity patterns.

- **An investment bank** was fined $500,000 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.

SAR Monitoring and Reporting Programs

FINRA Enforcement in 2025 also Highlighted Weaknesses in SAR Monitoring and Reporting Programs, including by taking action against alleged failures by AML Officers and CCOs.

- **A clearing broker-dealer** was subject to FINRA action after the firm failed to monitor for and report SAR at scale, resulting in the failure to file at least **218 SARs**. FINRA alleged that the firm's AML systems were not reasonably designed to detect or investigate red flags associated with suspicious trading and money movements, and that breakdowns in escalation and oversight undermined SAR reporting across its clearing business.
- **A broker-dealer** was fined $150,000 for alleged AML deficiencies related to its handling of exception reports used to identify suspicious activity. FINRA alleged that the firm routinely cleared transactions flagged by its clearing firm without documented review or escalation of red flags, reflecting weaknesses in SAR monitoring.
- **A broker-dealer** was fined $50,000 after FINRA found that the firm failed to monitor for and report SAR in its investment banking and M&A advisory business. FINRA alleged that, despite repeated examination findings and independent testing recommendations, the firm's WSPs still lacked business-specific red flags, continued to incorrectly disclaim SAR obligations, and relied on AML training focused on retail brokerage activity rather than advisory transactions.
- **A broker-dealer** was fined approximately $26 million after FINRA alleged that it failed to establish and implement **reasonable anti-money laundering (AML) programs**, causing the firm to fail to detect, investigate, or report suspicious activity; FINRA also found failures across supervisory systems, disclosures, and reporting obligations.

Compliance Best Practices

08

AML Compliance Programs: General Best Practices

Compliance program best practices:

- Regularly updated to ensure risk-based;
- Sufficient personnel, resources, and independence;
- Supported by adequate technology, including automation, as needed;
- Grows commensurate with business growth;
- Regularly tested and enforced;
- Compensation and promotion structures that reinforce and do not discourage compliance; and
- Supported by periodic and tailored training and a compliance tone from the top.

AML Compliance Programs: "Risk-Based" Approach

- Under the BSA, financial institutions should maintain a risk-based, written AML Program "reasonably designed" to prevent money laundering and terrorist financing and ensure compliance with applicable BSA requirements.
- FinCEN has suggested that a regularly updated risk assessment is important for a compliant AML program, including for new products, services, customer base, and geographic locations.
- Although regulators do not require the use of any particular technology or system, they encourage use of innovative technology to increase the efficacy of BSA/AML Programs.
- In April 2025, Acting Comptroller of the Currency Rodney Hood specifically mentioned banks using AI to help identify suspicious activity.

AML Compliance Programs: Additional Considerations

- Ongoing oversight for agents and counterparties, with monitoring.
- Mitigations related to anti-money laundering for specific products, such as transactional limits by and between senders and receivers.
- Information sharing with law enforcement, including participation in public-private partnership opportunities.
- Internal information sharing.
- Compliance involvement and review before mergers and acquisitions or integration of new products and services.

Sanctions & Export Compliance Programs: General Best Practices

Apply the OFAC compliance framework.

OFAC's 2019 *Framework for OFAC Compliance Commitments* identifies five essential components of a strong sanctions compliance program:

Recent enforcement actions continue to highlight the importance of maintaining a strong sanctions compliance program, such as restricted party and geolocation screening mechanisms designed to adequately address the risks of the business.

Look out for cross-agency guidance from OFAC, BIS, and partner agencies.

Recent cross-agency guidance from OFAC, BIS, and NSD ("Tri-Seal Note") underscores the importance of establishing strong and coordinated sanctions and export control compliance procedures.

Move quickly to investigate potential sanctions violations.

2025 enforcement actions underscore the cost of ignoring red flags, risks related to acquisitions, and failure to keep compliance programs commensurate with global risks.

Carefully weigh whether to self-disclose potential violations to NSD & BIS.

Sanctions & Export Control Compliance Programs: Implications for Financial Institutions

- Joint Agency Guide has affirmed that financial institutions (FIs) must comply with sanctions programs and export controls, **including General Prohibition 10** which prohibits:
  - Financing or servicing any item subject to U.S. export controls with knowledge or reason to know a violation of export controls has occurred or will occur.
  - Financing or facilitating certain activities with knowledge or reason to know they involve weapons of mass destruction or military-intelligence programs.
- FIs are being required to create more **robust programs that do not overly rely on information provided by exporters** to comply with sanctions and export controls.
- Financial institutions should adopt a **more integrated approach to compliance that crosses regulatory focus areas.** Moreover, FIs can decrease risk by:
  - Adopting a risk-based approach that appropriately weighs cross-border elements, foreign persons, and inconsistent transactional activity;
  - Enhancing minimum sanctions compliance expectations for co-parties, such as customer onboarding and ongoing due diligence standards; and
  - Using or developing AI and automated systems that (i) automatically communicate information between participating institutions and (ii) allow the system to pause suspect transactions for further review (e.g., exception processing),
  - Among other measures.

Upcoming February Programs

2025/2026 White Collar Webcast Series

Date and Time	Program	Registration Link
Thursday, February 5, 2026 **9:00 a.m. – 10:00 a.m. PT** **12:00 p.m. – 1:00 p.m. ET**	**Managing Third-Party Risk in a Shifting Regulatory Landscape** Presenters: Victor Tong, Oleh Vretsona, Ulla Pentinpuro (Principal, Control Risks), Michele Wiener (Partner, Control Risks)	Event Details
Tuesday, February 24, 2026 **9:00 a.m. – 10:00 a.m. PT** **12:00 p.m. – 1:00 p.m. ET**	**Commodities Enforcement and the CFTC** Presenters: David Burns, Amy Feagles, Jeffrey Steiner	Event Details
Thursday, February 26, 2026 **9:00 a.m. – 10:30 a.m. PT** **12:00 p.m. – 1:30 p.m. ET**	**State AG Developments** Presenters: Winston Chan, Christopher Chorba, Karin Portlock, Prerak Shah, Eric Vandevelde	Event Details

Attorney Bios

1700 M Street, N.W., Washington, D.C. 20036-4504

+1 202.887.3609

fwarin@gibsondunn.com

F. Joseph Warin

Partner / Washington, D.C.

F. Joseph Warin is chair of the 250-person Litigation Department of Gibson Dunn's Washington, D.C. office, and he is co-chair of the firm's global White Collar Defense and Investigations Practice Group. Joe's practice includes representation of corporations in complex civil litigation, white collar crime, and regulatory and securities enforcement – including Foreign Corrupt Practices Act investigations, False Claims Act cases, special committee representations, compliance counseling and class action civil litigation.

Joe is continually recognized annually in the top-tier by *Chambers USA*, *Chambers Global*, and *Chambers Latin America* for his FCPA, fraud and corporate investigations expertise. *Lexology Index* (formerly *Who's Who Legal*) named Joe a "Global Elite Thought Leader" in its Investigations guides list for Business Crime Defense – Corporate and Investigations each year since 2018, and also recognized him in its *Commercial Litigation 2023* guide. In 2021 *Global Investigations Review* named Joe to its list of Top FCPA Practitioners, which "highlights 30 outstanding lawyers and forensic advisers in the Foreign Corrupt Practices Act space." In 2022, Joe was selected by *Chambers USA* as a "Star" in FCPA, a "Leading Lawyer" in the nation in Securities Regulation: Enforcement, and a "Leading Lawyer" in the District of Columbia in Securities Litigation and White Collar Crime and Government Investigations. In 2017, *Chambers USA* honored Joe with the Outstanding Contribution to the Legal Profession Award, calling him a "true titan of the FCPA and securities enforcement arenas." He has been listed in *The Best Lawyers in America*® every year from 2006–2026 for White Collar Criminal Defense. *The U.S. Legal 500* ranks Joe in the 2025 Hall of Fame for Dispute Resolution – Corporate Investigations and White-Collar Criminal Defense, and he was most recently recommended for Securities Litigation: Defense. *Legal 500* has also repeatedly named him as a "Leading Lawyer" for Corporate Investigations and White Collar Criminal Defense Litigation.

Joe has handled cases and investigations in more than 40 states and dozens of countries. His clients include corporations, officers, directors and professionals in regulatory, investigative and trials involving federal regulatory inquiries, criminal investigations and cross-border inquiries by dozens of international enforcers, including UK's SFO and FCA, and government regulators in Germany, Switzerland, Hong Kong, and the Middle East. His credibility at DOJ and the SEC is unsurpassed among private practitioners – a reputation based in large part on his experience as the only person ever to serve as a compliance monitor or counsel to the compliance monitor in three separate FCPA monitorships, pursuant to settlements with the SEC and DOJ: Statoil ASA (2007-2009); Siemens AG (2009-2012); and Alliance One International (2011-2013).

Joe's full biography can be viewed here.

EDUCATION

Georgetown University
Juris Doctor

Creighton University
Bachelor of Arts

CLERKSHIPS

U.S.D.C., Eastern District of Virginia

1700 M Street, N.W., Washington, D.C. 20036-4504

+1 202.887.3502

sbrooker@gibsondunn.com

Stephanie Brooker

Partner / Washington, D.C.

Stephanie L. Brooker, a partner in Washington D.C. office of Gibson, Dunn & Crutcher, is Co-Chair of the firm's White Collar Defense and Investigations, Anti-Money Laundering, and Financial Institutions Practice Groups. Prior to joining the firm, Stephanie served as a prosecutor at the U.S. Department of Justice. As a DOJ prosecutor, Stephanie served as the Chief of the Asset Forfeiture and Money Laundering Section in the U.S. Attorney's Office for the District of Columbia, investigated a broad range of white collar and other federal criminal matters, tried 32 criminal trials, and briefed and argued criminal appeals. Stephanie also served as the Director of the Enforcement Division and Chief of Staff at the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN), the lead U.S. anti-money regulator and enforcement agency.

During her approximately 25 years in legal practice, Stephanie has been consistently recognized as a leading practitioner in the areas of anti-money laundering compliance and enforcement defense and white collar criminal defense. She was most recently recommended by The Legal 500 for her work in white collar defense and financial services-related matters. Chambers USA has ranked her and described her as an "excellent attorney," who clients rely on for "important and complex" matters, and noted that she provides "excellent service and terrific lawyering." Stephanie has also been named a National Law Journal White Collar Trailblazer, a Global Investigations Review Top 100 Women in Investigations, and an NLJ Awards Finalist for Professional Excellence—Crisis Management & Government Oversight.

Stephanie's practice focuses on internal investigations, regulatory enforcement defense, white-collar criminal defense, and compliance counseling. She handles a wide range of white collar matters, including representing financial institutions, boards of directors, multi-national companies, and individuals in connection with criminal and regulatory enforcement actions involving anti-money laundering (AML)/Bank Secrecy Act (BSA); sanctions; anti-corruption; digital assets and fintech; securities, tax, and wire fraud, foreign influence; work place misconduct; and other legal issues. She routinely handles complex cross-border investigations. Stephanie's practice also includes BSA/AML and FCPA compliance counseling and deal due diligence and significant criminal and civil asset forfeiture matters.

Stephanie's investigations matters involve multiple government agencies, including the Department of Justice (DOJ), Securities and Exchange Commission (SEC), Federal Reserve Board (FRB), Office of Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Office of Foreign Assets Control (OFAC), New York Department of Financial Services (NYDFS), Financial Industry Regulatory Authority (FINRA), state banking agencies and gaming regulators, and foreign regulators.

Stephanie's full biography can be viewed here.

EDUCATION

Georgetown University
Juris Doctor

Northwestern University
Bachelor of Science

CLERKSHIPS

U.S. Court of Appeals, 4th Circuit

U.S.D.C., District of Columbia

1700 M Street, N.W., Washington, D.C. 20036-4504

+1 202.887.3786

dburns@gibsondunn.com

David P. Burns

Partner / Washington, D.C.

David P. Burns is a litigation partner in the Washington, D.C., office of Gibson, Dunn & Crutcher. He is the co-chair of the firm's National Security Practice Group, and a member of the White Collar and Investigations and Crisis Management practice groups. His practice focuses on white-collar criminal defense, internal investigations, national security, and regulatory enforcement matters. David represents corporations and executives in federal, state, and regulatory investigations involving securities and commodities fraud, sanctions and export controls, theft of trade secrets and economic espionage, the Foreign Agents Registration Act, accounting fraud, the Foreign Corrupt Practices Act, international and domestic cartel enforcement, health care fraud, government contracting fraud, and the False Claims Act.

Prior to re-joining the firm, David served in senior positions in both the Criminal Division and National Security Division of the U.S. Department of Justice. Most recently, he served as Acting Assistant Attorney General of the Criminal Division, where he led more than 600 federal prosecutors who conducted investigations and prosecutions involving securities fraud, health care fraud, Foreign Corrupt Practices Act violations, public corruption, cybercrime, intellectual property theft, money laundering, Bank Secrecy Act violations, child exploitation, international narcotics trafficking, human rights violations, organized and transnational crime, gang violence, and other crimes, as well as matters involving international affairs and sensitive law enforcement techniques.

Prior to joining the Criminal Division, David served as the Principal Deputy Assistant Attorney General of the National Security Division from September 2018 to December 2020. In that role, he supervised the Division's investigations and prosecutions, including counterterrorism, counterintelligence, economic espionage, cyber hacking, FARA, disclosure of classified information, and sanctions and export controls matters. He also spent five years as an Assistant United States Attorney in the Southern District of New York, Criminal Division, from 2000 to 2005.

David's full biography can be viewed here.

EDUCATION

Georgetown University
Juris Doctor

Boston College
Bachelor of Arts

1700 M Street, N.W., Washington, D.C. 20036-4504

+1 202.955.8220

kday@gibsondunn.com

M. Kendall Day

Partner / Washington, D.C.

M. Kendall Day is a nationally recognized white-collar partner in the Washington, D.C. office of Gibson, Dunn & Crutcher, where he is Co-Chair of Gibson Dunn's Fintech and Digital Assets Practice Group, Co-Chair of the firm's Financial Institutions Practice Group, co-leads the firm's Anti-Money Laundering practice, and is a member of the White Collar Defense and Investigations and Crisis Management Practice Groups.

His practice focuses on internal investigations, regulatory enforcement defense, white-collar criminal defense, and compliance counseling. He represents financial institutions; fintech, digital asset, and multi-national companies; and individuals in connection with criminal, regulatory, and civil enforcement actions involving anti-money laundering (AML)/Bank Secrecy Act (BSA), sanctions, FCPA and other anti-corruption, securities, tax, wire and mail fraud, unlicensed money transmitter, false claims act, and sensitive employee matters. Kendall's practice also includes BSA/AML compliance counseling and due diligence, and the defense of forfeiture matters.

Prior to joining Gibson Dunn, Kendall had a distinguished 15-year career as a white collar prosecutor with the Department of Justice (DOJ), rising to the highest career position in the DOJ's Criminal Division as an Acting Deputy Assistant Attorney General (DAAG). As a DAAG, Kendall had responsibility for approximately 200 prosecutors and other professionals. Kendall also previously served as Chief and Principal Deputy Chief of the Money Laundering and Asset Recovery Section. In these various leadership positions, from 2013 until 2018, Kendall supervised investigations and prosecutions of many of the country's most significant and high-profile cases involving allegations of corporate and financial misconduct. He also exercised nationwide supervisory authority over the DOJ's money laundering program, particularly any BSA and money-laundering charges, deferred prosecution agreements and non-prosecution agreements involving financial institutions.

Earlier in his time as a white collar prosecutor, from 2005 until 2013, Kendall served as a deputy chief and trial attorney in the Public Integrity Section of the DOJ. During his tenure at the Public Integrity Section, Kendall prosecuted and tried some of the Criminal Division's most challenging cases, including the prosecutions of Jack Abramoff, a Member of Congress and several chiefs of staff, a New York state supreme court judge, and other elected local officials. He started his career in 2003 when he was selected to join the Attorney General's Honors Program as a prosecutor in the DOJ's Tax Division.

Kendall's full biography can be viewed here.

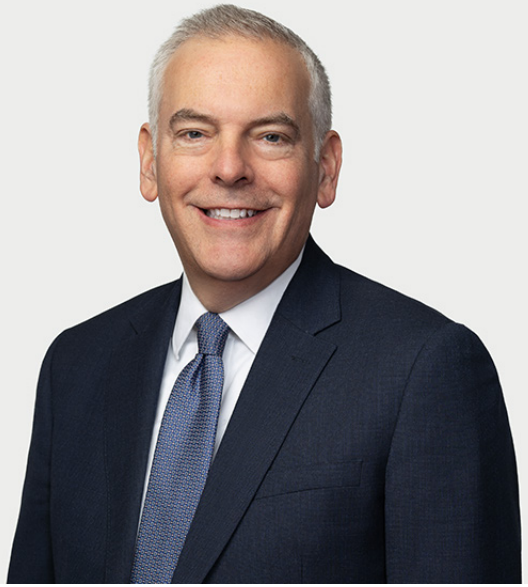
EDUCATION

University of Virginia
Juris Doctor

University of Kansas
Bachelor of Arts

CLERKSHIPS

U.S.D.C., Maryland



1700 M Street, N.W., Washington, D.C. 20036-4504

+1 202.955.8517

maxelrod@gibsondunn.com

Matthew S. Axelrod

Partner / Washington, D.C.

Matt is a nationally recognized crisis management and white-collar defense lawyer with deep criminal, national security, and export enforcement experience. His practice focuses on internal investigations, white-collar criminal defense, and crisis management for U.S. and multinational companies, their boards, and their senior executives. Matt co-chairs Gibson Dunn's Sanctions and Export Enforcement practice, where he works closely with clients to conduct internal investigations, evaluate compliance programs, advise on voluntary self-disclosures, and defend against government-facing investigations.

Matt is the only person to have previously served as both Principal Associate Deputy Attorney General at the U.S. Department of Justice — a role described in the *New York Times* "as the most demanding job in all of DOJ" – and Assistant Secretary for Export Enforcement at the U.S. Department of Commerce's Bureau of Industry and Security (BIS). His over 25 years of government enforcement, white-collar defense, and crisis management experience are why clients consistently rely on Matt to help them navigate their most sensitive and complex matters. *Lawdragon* recently named Matt as one of the 500 Global Leaders in Crisis Management.

Immediately before joining Gibson Dunn, Matt served as the Senate-confirmed Assistant Secretary for Export Enforcement at BIS, where he led the team responsible for enforcing the country's export control and antiboycott laws. During Matt's tenure, BIS brought a record number of criminal and administrative enforcement actions, including the highest standalone administrative penalty in the agency's history. Matt revamped the agency's export enforcement policies (including those on voluntary self-disclosures), issued numerous compliance guidance memos for industry, launched the boycott requester list, and was an architect of the Disruptive Technology Strike Force. Prior to his confirmation, Matt served as Special Counsel in the White House Counsel's Office, where he advised on national security and domestic issues.

Matt also spent over thirteen years at the Department of Justice, including serving twice as Principal Associate Deputy Attorney General. Alongside the Deputy Attorney General, Matt oversaw DOJ's entire workforce, including the prosecutors and agents in the U.S. Attorney's Offices, the Criminal Division, the National Security Division, and the FBI. Matt also provided oversight of all significant corporate enforcement resolutions, managed countless crises, and engaged with Congress and the White House on DOJ's behalf.

Matt's full biography can be viewed here.

EDUCATION

Yale University
Juris Doctor

Amherst College
Bachelor of Arts

CLERKSHIPS

U.S.D.C., Connecticut

U.S. Court of Appeals, 2nd Circuit

1700 M Street, N.W., Washington, D.C. 20036-4504

+1 202.887.3511

ecapone@gibsondunn.com

Ella Alves Capone

Of Counsel / Washington, D.C.

Ella Alves Capone is of counsel in the Washington, D.C. office of Gibson, Dunn & Crutcher. She is a member of the White Collar Defense and Investigations, Financial Regulatory, FinTech and Digital Assets, and Anti-Money Laundering Practice Groups.

Ella has been featured as a fintech "Rising Star" by *Law360* in its 2023 publication of "attorneys under 40 whose legal accomplishments belie their age." She has also been recognized by *Super Lawyers* as a 2022 and 2023 White Collar Defense "Rising Star." In addition, she was recognized for her White Collar Litigation and Investigations work in the 2023 *Lawdragon 500 X – The Next Generation* edition, an inaugural guide highlighting attorneys "who will define where the legal profession of our country goes" and whose "leadership will be called upon by businesses and individuals when they face their crossroads."

Ella's practice focuses on advising multinational corporations and financial institutions on Bank Secrecy Act/anti-money laundering (BSA/AML), anti-corruption, sanctions, payments, and consumer financial regulatory and enforcement matters, with a particular focus on regulatory matters impacting banks, casinos, social media and gaming platforms, marketplaces, fintech, payment service providers, and digital assets businesses. She regularly advises clients on the implementation, enhancement, and assessment of their compliance programs and internal controls and on platform terms and conditions, including Terms of Service, Merchant Agreements, Sales Agreements, Payment and Refund Policies, and Payment Service Provider Agreements. Ella frequently provides clients with training on financial services regulations and corporate compliance programs, including enforcement trends, industry best practices, and regulator expectations.

Ella has significant experience representing clients in white collar and regulatory matters involving the Department of Justice (DOJ), Securities Exchange Commission (SEC), Financial Crimes Enforcement Network (FinCEN), Office of the Comptroller of the Currency (OCC), Office of Foreign Assets Control (OFAC), the Federal Reserve, and state financial services regulators, including the New York State Department of Financial Services (DFS). She has successfully defended global clients in multi-jurisdictional and multi-agency enforcement matters involving Foreign Corrupt Practices Act (FCPA), AML, consumer financial, securities, fraud, and sanctions allegations.

Ella's full biography can be viewed here.

EDUCATION

New York University
Juris Doctor

Fordham University
Bachelor of Science

200 Park Avenue, New York, NY 10166-0193

+1 212.351.2499

sraymond@gibsondunn.com

Sam Raymond

Of Counsel / New York

Sam Raymond is Of Counsel in the New York office of Gibson Dunn & Crutcher and a member of the White Collar Defense and Investigations, Litigation, Anti-Money Laundering, Fintech and Digital Assets, and National Security Groups. As a former federal prosecutor, Sam has a broad-based government enforcement and investigations practice, with a specific focus on investigations and counseling related to anti-money laundering, the Bank Secrecy Act, and sanctions.

Sam is an experienced investigator and trial lawyer. Prior to joining Gibson Dunn, Sam was an Assistant United States Attorney in the U.S. Attorney's Office for the Southern District of New York from 2017 to 2024. In that role, Sam tried multiple cases to verdict and prosecuted a broad range of federal criminal violations. Sam was a member of the team that prosecuted executives at FTX and Alameda Research, including as a member of the trial team in *United States v. Bankman-Fried*, and was the lead prosecutor in the FTX case on issues related to asset seizure and forfeiture. Sam was also a member of the DOJ team that brought criminal charges against the senior leadership of Hamas for their roles in planning, supporting and perpetrating the October 7 terrorist attacks on Israel. Sam was a lead prosecutor in one of the first cases ever charging individuals with violations of the Bank Secrecy Act, in a pathbreaking prosecution of executives at a cryptocurrency exchange.

Sam led dozens of other investigations and prosecutions, including in cases involving money laundering, unlicensed money transmitting, sanctions evasion, asset seizure and forfeiture, tax fraud, securities fraud, bank and wire fraud, racketeering, extortion, illicit gambling, art fraud, and government benefits fraud. Earlier in his career, Sam prosecuted cases involving gang violence and narcotics trafficking. Sam argued multiple times before the Second Circuit Court of Appeals, including with respect to constitutional issues of first impression. He also served as one of the Office's inaugural Digital Asset Coordinators, offering trainings and coordinating within the Office regarding digital assets, and engaging with other U.S. Attorney's Offices, Department of Justice components, and law enforcement agencies, regarding cryptocurrency.

Prior to his government service, Sam practiced for several years at another major international law firm, where he practiced white collar defense and litigated complex civil cases and appeals.

Sam's full biography can be viewed here.

EDUCATION

New York University
Juris Doctor

Massachusetts Institute of Technology
Bachelor of Science

CLERKSHIPS

U.S. Court of Appeals, 9th Circuit

U.S.D.C., Central District of California

1700 M Street, N.W., Washington, D.C. 20036-4504

+1 202.887.3509

ssewall@gibsondunn.com

Samantha Sewall

Of Counsel / Washington, D.C.

Samantha Sewall is of counsel in the Washington, D.C. office of Gibson, Dunn & Crutcher and a member of the firm's International Trade Practice Group.

She advises clients on compliance with U.S. legal obligations at the intersection of global trade, foreign policy, and national security, focusing her practice on compliance with U.S. economic sanctions, export controls, national security reviews of foreign direct investment (CFIUS), and anti-boycott laws. Samantha has experience advising companies across a wide range of sectors including aerospace, banking and financial institutions, defense, energy, medical devices and pharmaceuticals, shipping, retail, telecommunications, and travel.

On a *pro bono* basis, Samantha has assisted clients with understanding U.S. trade controls and immigration issues, and she has worked with an international rule of law NGO to support law enforcement training efforts to combat transnational human trafficking and forced labor.

Prior to joining Gibson Dunn, she served as a Political-Economic Program Assistant supporting the U.S. Embassy in Côte d'Ivoire. During her time there she was responsible for programs and research related to private sector engagement and bilateral political and economic issues. Samantha was previously an associate with a large international law firm where she was a member of the international trade and investment practice group.

Samantha graduated *magna cum laude* from Georgetown University Law Center in 2012, where she was elected to the Order of the Coif and was a member of the *Georgetown Law Journal*. She is admitted to practice in the Commonwealth of Virginia, the District of Columbia, and the U.S. Court of International Trade.

Samantha's full biography can be viewed here.

EDUCATION

Georgetown University
Juris Doctor

Patrick Henry College
Bachelor of Arts

GIBSON DUNN