

**IPO and Public Company Readiness: Advance Planning
for 2025 and 2026 IPOs**

Regulatory Considerations for Public Companies and Their Key Stakeholders

January 15, 2025

GIBSON DUNN

Today's Speakers



Cynthia Mabry

Partner, Houston



Adam Smith

Partner, Washington, D.C.



Patrick Stokes

Partner, Washington, D.C.



Sam Raymond

Of Counsel, New York

TABLE OF CONTENTS

01 Overview

02 Office of Foreign Assets Control (OFAC) and FinCEN

03 Anti-Money Laundering (AML)

04 Foreign Corrupt Practices Act (FCPA)

05 Compliance Considerations

06 Sustainability and DE&I

MCLE Certificate Information

The information in this presentation has been prepared for general informational purposes only. It is not provided in the course of an attorney-client relationship and is not intended to create, and receipt does not constitute, an attorney-client relationship or legal advice or to substitute for obtaining legal advice from an attorney licensed in the appropriate jurisdiction.

This presentation has been approved for **1 General credit**.

- Participants must submit the form by **Wednesday, January 22nd** in order to receive CLE credit.
- Most participants should anticipate receiving their certificate of attendance in 4-6 weeks following the webcast.
- All questions regarding MCLE Information should be directed to CLE@gibsondunn.com

Overview

01

Overview

- “White Collar” enforcement has been a significant focus for DOJ/SEC/Treasury in recent years.
- Investment banks are **heavily scrutinized** under AML/FCPA/OFAC regulations.
 - Regulators expect investment banks to act as a “gatekeeper” and conduct due diligence on the companies for whom they act as underwriter.
 - Compliance issues for an IPO company can result in regulatory scrutiny and reputational harm for underwriters as well as the IPO company.
- Compliance issues are therefore a focus of both due diligence and representations and warranties.



Risks From a Compliance Issue

Damage to Business

- Damage to Reputation
- Diverted Management and Board Focus
- Direct Response Costs

Litigation/Regulatory Risks

- Law Enforcement Investigations (e.g., DOJ)
- Regulatory Investigations (e.g., SEC/OFAC/FinCEN)
- Derivative/Shareholder Actions

Impact to Company/Stock Price

- Loss of Investor Confidence
- Negative Financial Impact

Key IPO Considerations

Disclosure

- Registration statement/prospectus must appropriately disclose material risks regarding compliance efforts/issues.

Underwriters' due diligence

- Underwriters seeking to establish due diligence defense AND meet expectations of their own regulators by conducting reasonable diligence.
- Underwriters will expect focused representations and warranties in underwriting agreement.

Public attention

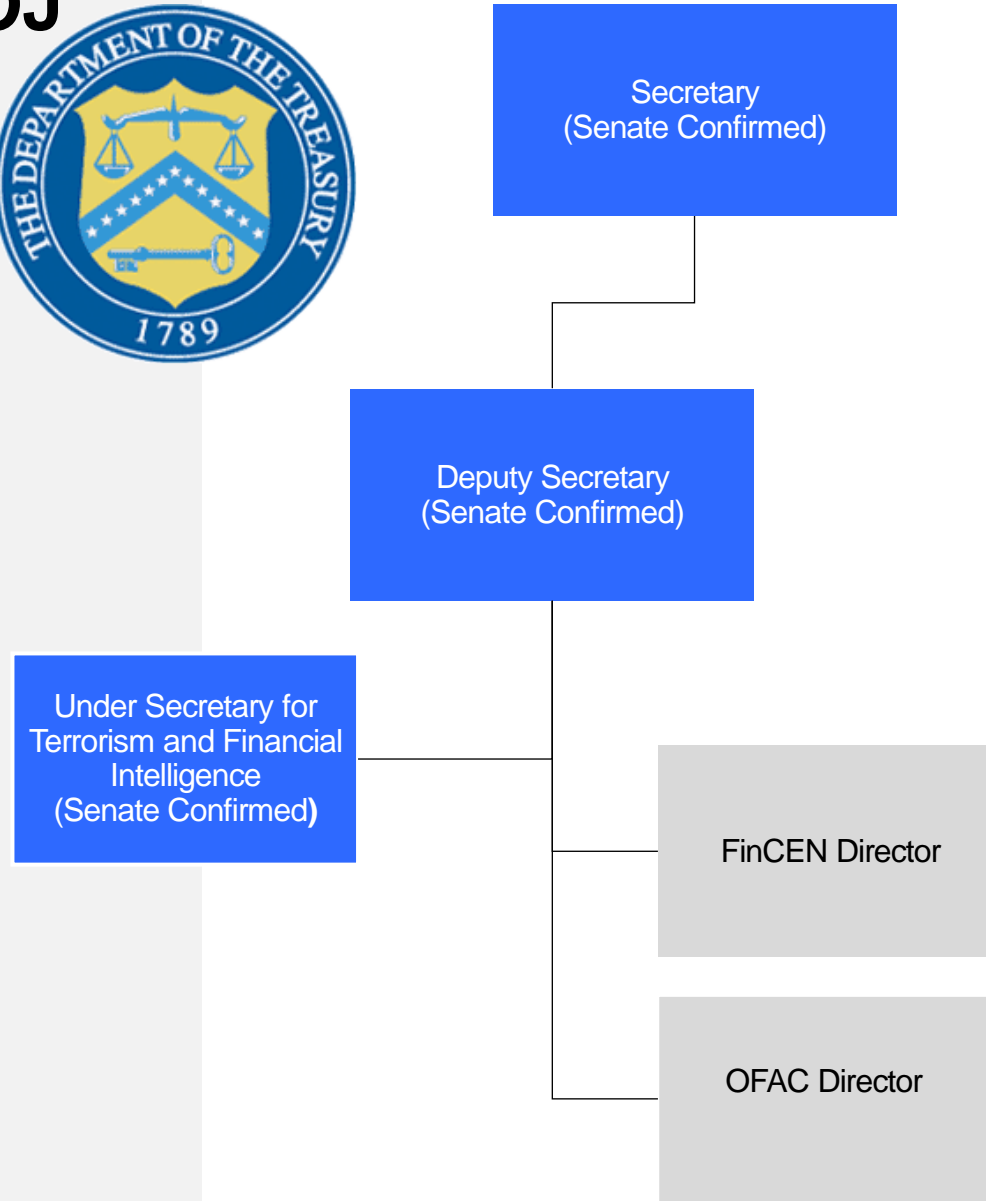
- Publicity around IPO/being a public company may attract higher level of scrutiny.

Office of Foreign Assets Control (OFAC) and FinCEN

02

Treasury and DOJ

Key Personnel



Three Types of Sanctions



*Sanctions compliance is important to underwriters, investors, business partners because many prohibitions under U.S. sanctions apply on a **strict liability basis** and **do not necessarily take corporate formality into account.***

Primary Sanctions

1

Comprehensive Sanctions

- Cuba
- Iran
- North Korea
- Syria
- Crimea
- Donetsk People's Republic ("DNR")
- Luhansk People's Republic ("LNR")

2

List-Based Sanctions

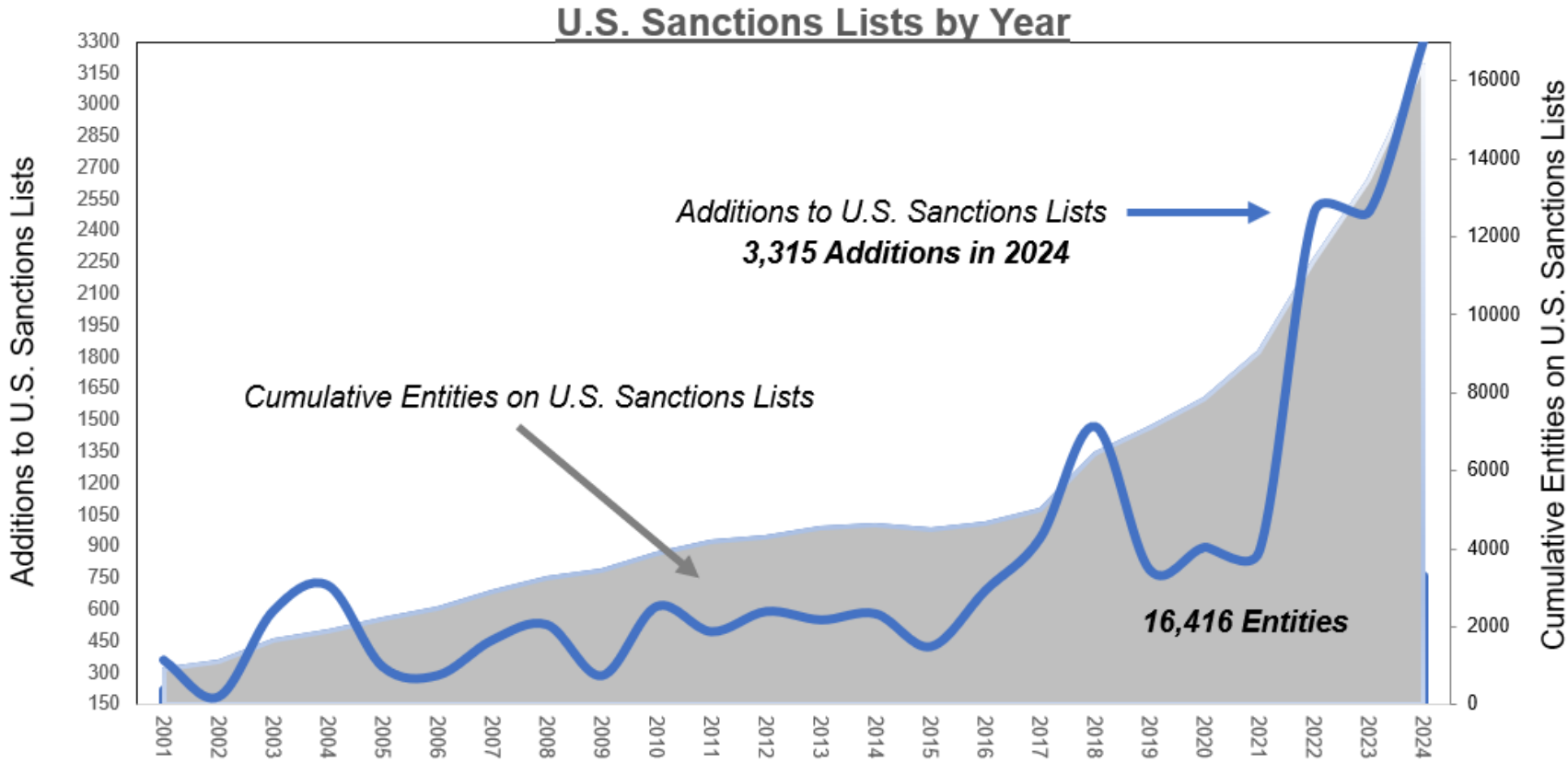
- Blocking Sanctions
- Sectoral Sanctions
- 50% Rule

3

Secondary Sanctions

- Iran
- Russia
- North Korea
- Syria
- Hong Kong

List-Based Sanctions



Source: U.S. Treasury Department data compiled by Adam Smith of Gibson Dunn

- **Target “bad guys”** (terrorism, weapons proliferation, narcotics trafficking, human rights abuses, corruption, etc.)
- Can be individuals, entities, vessels, aircraft
- **Various OFAC restricted party lists**
- Prohibit all, or only certain specific types of, transactions involving targeted parties
- **Specially Designated Nationals (“SDNs”)**
- Complete prohibition; no transactions or dealings in any way involving an SDN without authorization
- Requirement to block property and report

Treasury's Stance on Sanctions Issues

Throughout 2024, the Biden Administration leveraged its sanctions toolbox to put economic pressure on countries including Russia, Iran, China, and North Korea in order to further its foreign policy and national security goals. We expect the Trump Administration to continue aggressive use of sanctions.



Ukraine's success is in America's core national interest. Stopping Russia's illegal invasion will help uphold a global democratic, rules-based, order that advances American security and economic interests, and it will send an unmistakable message to autocrats and would-be aggressors around the world that they will face unshakeable resolve."

Janet L. Yellen
Secretary of the Treasury
December 30, 2024

"Iran continues to rely on its shadowy network of vessels, companies, and facilitators to finance the development of its nuclear program, the proliferation of its weapons systems, and support to its proxies. The United States is committed to targeting Iran's key revenue streams that fund its destabilizing activities."

Bradley T. Smith
Acting Under Secretary of the Treasury for Terrorism &
Financial Intelligence
December 19, 2024



Three Primary Sanctions Risks

Best-Practice Compliance Needs to Simultaneously Cover Each Risk

The growth of sanctions programs adds to the number and type of sanctionable conduct and increases the potential of being listed.

1 Black-Listing

Governments can list a bank or a company for engaging in sanctionable conduct and bar them from access to their jurisdiction. The consequences of being listed are severe: assets are frozen and access to markets—retail, investment, insurance, bonds, reinsurance, and correspondent banking—restricted or prohibited.

The large number of enforcement agencies involved, and the ever-growing number of black-listed entities, increases the likelihood of engaging with sanctioned parties.

2 Penalties

A company that even accidentally engages with black-listed parties can face reputational, civil, and criminal liability—for itself and its officers and directors. Authorities have assessed billions of dollars of fines, required divestment of state funds from companies, mandated post-settlement monitoring, and suspended operating licenses.

The rising risks of being black-listed and penalized—combined with reputational harm—means that no firms are “too big to be de-risked.”

3 De-Risking

A bank or a company can face sanctions-related consequences if its business partners are concerned that its compliance is unsatisfactory. Dozens of major firms have “de-risked”—cutting off customers, licensees, bankers, investors, and even whole lines of business due to perceived direct or indirect sanctions exposure.

Complying with U.S. Sanctions: Developing and Deploying Policies & Procedures

- An adequate sanctions compliance program will often include:
 - Counterparty “**screening**” tools that compare counterparty information, including ultimate beneficial owners, **against the SDN List** and other relevant restricted party lists
 - Procedures for **escalating transactions that pose an unacceptable risk** of violating applicable sanctions for further review
 - Internet Protocol address-based **geo-blocking** to prevent **persons in sanctioned jurisdictions** from accessing a company’s online platform or products.
- It is also often necessary to develop related policies and procedures to **review, record, and potentially report transactions** that appear to have violated sanctions
- Additionally, some companies must maintain adequate policies and procedures to **classify items and, if applicable, fulfill the reporting requirements under the Export Administration Regulations** (i.e., “export controls”).
 - Export controls and sanctions are oftentimes interrelated, and so export controls compliance programs may respond to some of the same concerns animating sanctions compliance.

The U.S. “Sanctions” Policy Dials:

Diversity of Tools, Authorities, and Agencies

1

Economic Sanctions

Agency
Treasury Dept.

Legal Basis
IEEPA, TWEA, and others

Examples
Sanctions re HK and XUAR

2

Export Controls

Agency
Commerce & State Depts.

Legal Basis
Export Control Reform Act,
Arms Export Control Act

Examples
Limits on tech exports

3

Tariffs

Agency
USTR

Legal Basis
Tariff Act of 1974, others

Examples
Section 301, Section 232

4

Import Controls

Agency
Homeland Security Dept.

Legal Basis
Various

Examples
UFLPA

5

FDI Controls

Agency
Treasury lead – 9 agencies

Legal Basis
FIRRMA, Exon-Florio

Examples
Review / Rejection of FDI

6

“Reverse” CFIUS

Agency
Treasury Dept. – new Office
of Global Transactions

Legal Basis
Executive Action

Examples
Notification or prohibition of
Outbound Flows

Enforcement Guidelines

Base Penalty – Calculated per Transaction

- Egregious?
- Voluntarily self-disclosed?

Mitigating and Aggravating Factors

- Willful or reckless
- Awareness of conduct
- Management involvement
- Pattern of conduct and repeat violations
- Harm to sanctions program objectives
- Volume of transactions
- Size and sophistication of violating person
- Existence and adequacy of compliance program
- Remedial response
- Cooperation

		Egregious Case	
		NO	YES
Voluntary Self-Disclosure	YES	(1) One-Half of Transaction Value (capped at <u>lesser</u> of \$184,068 or one-half of the applicable statutory maximum per violation)	(3) One-Half of Applicable Statutory Maximum
	NO	(2) Applicable Schedule Amount (capped at <u>lesser</u> of \$368,136 or the applicable statutory maximum per violation)*	(4) Applicable Statutory Maximum

Current as of January 15, 2025, civil monetary penalties available under IEEPA include \$377,700 per transaction or twice the value of the underlying transaction, whichever is greater.

**As of 9:00 AM, January 15, 2025, OFAC has not yet updated its Base Penalty Matrix to reflect the 2025 inflation adjustment to IEEPA civil monetary penalties 17*

OFAC Monetary Penalties

Civil Penalties

	Total Penalties	# Actions
2012	\$1,139,158,727	16
2013	\$137,075,560	27
2014	\$1,205,225,807	22
2015	\$599,705,997	15
2016	\$21,609,315	9
2017	\$119,527,845	16
2018	\$71,510,561	7
2019	\$1,289,027,059	26
2020	\$23,565,657	16
2021	\$20,896,739	20
2022	\$42,664,006	16
2023	\$1,541,380,594.08	17
2024	\$48,790,404	12

Significant Fines

	Organization	Penalty Amount
2023	Binance	\$968,618,825
2014	BNP Paribas SA	\$963,619,900
2019	Standard Chartered Bank	\$657,040,033
2012	ING Bank N.V.	\$619,000,000
2019	UniCredit Bank AG	\$611,023,421
2023	British American Tobacco p.l.c.	\$508,612,492
2015	Crédit Agricole Corporate	\$329,593,585

- The OFAC monetary penalties only tell a portion of the story. Other U.S. regulators and enforcement agencies such as the DOJ, SEC, NYDFS and others may also impose penalties, disgorgement and forfeiture requirements.
- For example, BNP Paribas' total penalty calculation to settle its sanctions issues with the United States totaled nearly \$9 billion.

Anti-Money Laundering (AML)

03

U.S. AML and Sanctions Regulators and Enforcers

Primary AML and Sanctions Regulators



FinCEN



OFAC



State
Regulators

GIBSON DUNN

Secondary AML and Sanctions Regulators



Banking Regulators
(OCC, Fed,
FDIC, NCUA)



CFTC



SEC



FINRA

Enforcers



DOJ Criminal Division MLARS
National Security Division CES
U.S. Attorney's Offices
DOJ Civil Division CPB

AML Framework Criminal Provisions 18 U.S.C. §1956 and 1957

It is a crime to engage in a financial transaction with **knowledge** that the proceeds involved are the proceeds of unlawful activity, and the proceeds were derived from a specified unlawful activity.

- **Unlawful Activity** – Generally any violation of criminal law – federal, state, local or foreign
- **Specified Unlawful Activities** – Over 200 specified unlawful activities – U.S. and certain foreign crimes
- **Knowledge includes “willful blindness”** – Turning a blind eye or deliberately avoiding gaining positive knowledge when faced with a high likelihood of criminal activity, i.e., **ignoring red flags**
- **Scope** – Applies broadly to include corporate and individual enforcement of U.S. persons and individuals outside the U.S

AML Framework Provisions 31 U.S.C. § 5318

The Bank Secrecy Act, codified at 31 U.S.C. § 5318 and associated regulations, applies to “financial institutions,” including banks, broker dealers, money services businesses, casinos and others. Those institutions must implement an “anti-money laundering” program.

- **Regulation** – Different authorities enact BSA regulations for different types of financial institutions (OCC/FRB for banks, FinCEN for MSBs, SEC for broker-dealers).
- **Basic pillars** – Basic pillars of a compliant anti-money laundering program include:
 - a system of internal controls to ensure ongoing compliance
 - independent testing of BSA/AML compliance
 - the designation of an individual responsible for day-to-day compliance
 - training for appropriate personnel
 - customer due diligence.

AML Framework Provisions 31 U.S.C. § 5318 (cont'd)

- **“Risk Based”** – There are different rules that apply to different types of financial institutions. For example, while banks and broker dealers must have a “customer identification program” to identify all customers, money services businesses and investment advisers are not required to identify every customer.
- **“Risk Assessment”** – In keeping with the BSA’s focus on “risk,” FinCEN recently proposed a new rule which mandates a “risk assessment,” which would allow the institution to better identify and understand its exposure to money laundering, terrorist financing, and other illicit finance activity risks. Financial institutions would be expected to use the results of their risk assessment process to develop risk-based internal policies, procedures, and controls.

Violations of 31 U.S.C. § 5318

The Bank Secrecy Act carries a range of different penalties, depending on the type of institution and whether the institution acted “**willfully.**”

- **Negligent or reckless violations** – generally punished civilly, with fines, remediation, and sometimes monitorships.
 - Charges can be brought either by FinCEN or one of the supervisory state or federal regulators, or both.
 - FinCEN and other regulators can bring charges against both corporations and individuals.
 - Fines have exceeded hundreds of millions of dollars.

Violations of 31 U.S.C. § 5318 (cont'd)

- **Willful violations** – can be punished by FinCEN or other civil regulator with higher fines.
 - DOJ can also bring criminal charges, which can carry other collateral consequences and even greater fines.
 - DOJ can also bring charges against individuals.
 - Criminal BSA charges have become more prominent in the past few years, under both the first Trump and Biden Administrations.
 - Willful violations have led to corporations facing penalties in excess of \$1 billion, including recent total financial penalties of \$4.3 billion against a cryptocurrency exchange and \$3.1 billion against a bank.

Foreign Corrupt Practices Act (FCPA)

04

FCPA – Statute (15 U.S.C. §§ 78dd-1, 78dd-2, 78dd-3)

Anti-Bribery Provisions:

Prohibit corruptly giving, promising, or offering anything of value to a foreign government official, political party, or party official with the intent to influence that official in his or her official capacity or to secure an improper advantage in order to obtain or retain business.

Accounting Provisions:

Require issuers to (a) “make and keep books, records, and accounts, which in reasonable detail, accurately and fairly reflect the transactions and dispositions” of assets; and (b) “devise and maintain a system of internal accounting controls”

U.S. Enforcement Agencies

Department of Justice

- Criminal and civil enforcement of anti-bribery provisions (except issuers)
- Criminal enforcement of accounting provisions
- ~35 prosecutors in the Criminal Division



Securities and Exchange Commission

- Civil enforcement of the anti-bribery provisions (issuers)
- Civil enforcement of accounting provisions



FCPA (Anti-Bribery) - Elements of an Offense

It is illegal to . . .

- give, promise, offer, or authorize the provision of
- anything of value
- to a foreign government official
- directly or indirectly
- corruptly
- to influence the official in his or her official capacity or to secure an improper advantage in order to obtain or retain business

FCPA (Anti-Bribery) - “Anything of Value”

- Liability exists from the first dollar. There is **no “de minimis” exception.**
- It is **not limited to tangible items** of economic value.
- It can include **anything a recipient would find useful**, including:
 - Cash
 - Gifts
 - Entertainment
 - Food and wine
 - Meals
 - Internships
 - Professional training
 - Loans
 - Invitations to a conference
 - Event tickets
 - Political or charitable contributions
 - Travel
 - Employment
 - Consulting fees
 - Tuition

“A company must have “clear and easily accessible guidelines and processes in place for gift-giving by the company’s directors, officers, employees, and agents.”

[Resource Guide to the U.S. Foreign Corrupt Practices Act](#)

FCPA – Accounting Provisions

Books and Records

“[M]ake and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect transactions and dispositions of the assets” consistent with GAAP.

- The books and records provision applies to all transactions, not just FCPA payments.
- The SEC takes the position that a bribe must be described as a “bribe,” not a “payment,” “commission,” “incentive payment,” or “general fund.”

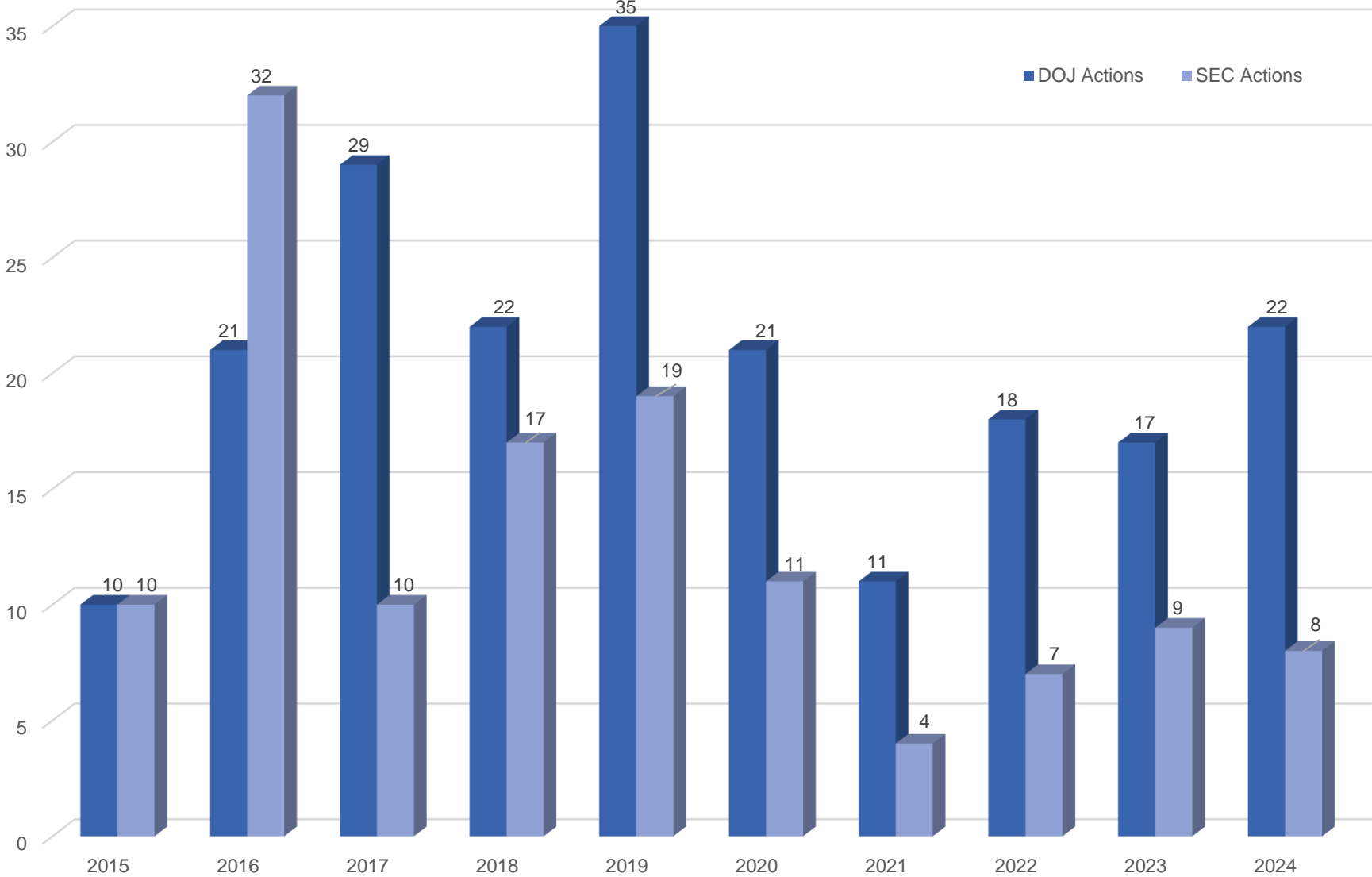
Internal Controls

Devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that—

- transactions are executed in accordance with management’s general or specific authorization
- transactions are recorded as necessary –
 - to permit preparation of financial statements in conformity with GAAP or any other criteria applicable to such statements and
 - to maintain accountability for assets.

FCPA Enforcement Actions Per Year

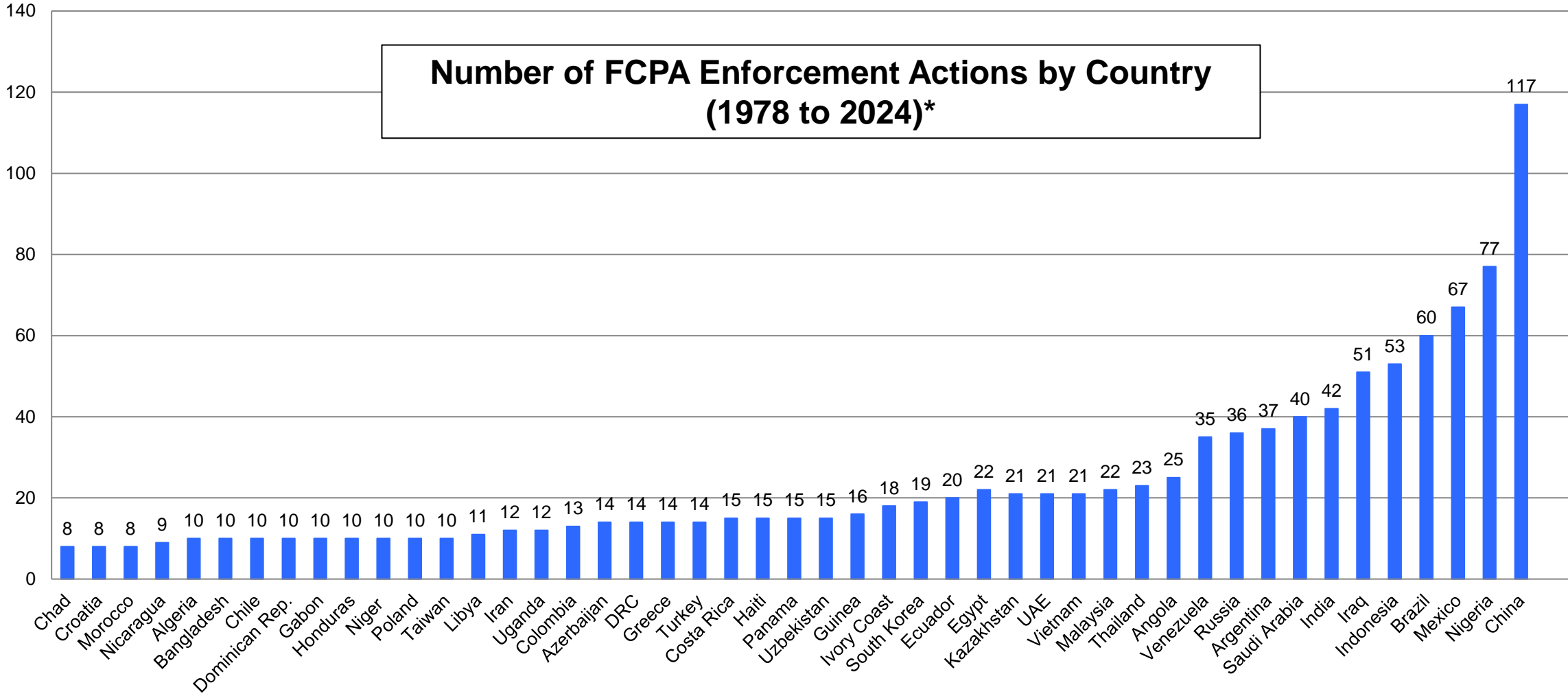
Number of FCPA Enforcement Actions Per Year



Largest Corporate FCPA Enforcement Actions

No.	Company	U.S. Penalties, Forfeiture, and Disgorgement	Year
1	Goldman Sachs	\$1.66 billion (\$1.263 billion DOJ, \$400 million SEC)	2020
2	Ericsson	\$1.27 billion (\$726 million DOJ, \$540 million SEC)	2019/2023
3	Mobile TeleSystems	\$850 million (\$750 million DOJ, \$100 million SEC)	2019
4	Siemens	\$800 million (\$450 million DOJ, \$350 million SEC)	2008
5	Alstom	\$772 million (DOJ)	2014
6	Glencore	\$701 million (DOJ)	2022
7	Gunvor	\$662 million (DOJ)	2024
8	KBR/Haliburton	\$579 million (\$402 million DOJ, \$177 million SEC)	2009
9	Teva Pharma	\$519 million (\$283 million DOJ, \$236 million SEC)	2016
10	Telia	\$483 million (\$275 million DOJ, \$208 million SEC)	2017

FCPA – Geographic Enforcement



* Minimum eight enforcement actions.

FCPA General Enforcement Trends

Common Fact Patterns in Enforcement Actions:

Certain high-risk areas and types of anti-corruption control breakdowns appear more often in FCPA resolutions:

- Disregarding red flags raised by due diligence, audit findings, and complaints
- Failure to implement recommendations from internal audit or legal
- Use of risky third-party intermediaries in connection with government-related business
 - Third-parties continue to pose the greatest FCPA risk and feature in enforcement actions.
- Deficiencies in global and/or post-deal compliance integration
- Departures from internal policies and procedures

Authorities will not credit companies for having internal controls if they are easily circumvented.

Trend: Third Parties Remain the Single Greatest Area of Corruption Risk

- **Albemarle Corporation:** On September 29, 2023, Albemarle Corporation, a chemical catalyst business, resolved investigations by SEC and DOJ into its participation in bribery schemes involving multiple foreign governments, agreeing to pay over USD 218 million in penalties and disgorgement. Albemarle allegedly made *payments through intermediaries* to secure business with state-owned oil companies in Vietnam, India, and Indonesia. Albemarle also allegedly made improper payments to private sector refineries in India.
- **H.W. Wood Limited:** On November 20, 2023, H.W. Wood Limited, a U.K.-based reinsurance broker, entered into a three-year DPA with DOJ and agreed to pay USD 508,000. According to the DPA, H.W. Wood allegedly *utilized a third-party intermediary to pay commissions* to three Ecuadorian officials and two Ecuadorian state-owned insurance companies to secure advantages in obtaining and retaining insurance and reinsurance business with the state-owned insurance entities.
- **Flutter:** On March 6, 2023, Flutter resolved an SEC-only FCPA enforcement action arising out of conduct in Russia. Irish sports betting and gaming company, Flutter, paid nearly USD 9 million to Russian consultants between 2015 and 2020 in an apparently unsuccessful effort to legalize online poker in the country. SEC alleged that Flutter *failed to perform risk-based diligence prior to hiring the consultants*. To resolve the FCPA books-and-records and internal controls charges, and without admitting or denying the findings, Flutter agreed to pay a USD 4 million civil penalty.

Mitigation: Carefully Monitor High-Risk Third Parties

Use of third parties is an inevitable part of doing business in an emerging market. Pre-engagement screening, as well as close monitoring, can help offset the decreased transparency and control that comes with using agents and intermediaries.

BEST PRACTICES

- ✓ Identify the specific functions *prone to corruption* that are handled by third parties.
- ✓ *Perform risk-based, anti-corruption due diligence* on any third-party agents prior to retention, and periodically refresh due diligence for higher-risk third parties.
- ✓ Involve *Legal and Compliance* in contract negotiations/drafting to ensure that services are specifically and accurately described and ensure that an efficient control (e.g., Finance) can assess whether the services have actually been rendered and whether prices are reasonable in light of those services and in line with market rates.
- ✓ Include *audit rights with a trigger* in third-party agreements to allow for audits when indicated.
- ✓ Conduct *specific training* for employees working with third parties and with end customers.
- ✓ Use a risk-based approach to periodically select third parties for an *audit review*.
- ✓ Ensure that *rebates, credit notes, and other payments* provided to the third party are made to the contracting entity, including identifying any offshore arrangements.
- ✓ Understand the *interaction* in emerging markets between sales force, third parties (e.g., distributors, agents), and end-customers, and conduct function-specific compliance training with these employees.
- ✓ Understand whether margins of intermediaries are *passed on* to end-customers by reviewing publicly available tender materials or conducting audit reviews.

Trend: **Enforcement Authorities’ Focus on M&A and the New M&A Safe Harbor Policy**

Part of the DOJ’s enhanced focus on timely, well-designed compliance programs and voluntary self-disclosures

Companies that voluntarily self-disclose misconduct at an acquired company within the Safe Harbor policy will receive a **presumption of a declination**

- Presumption of a declination -- DOJ’s decision not to prosecute a company

To qualify, companies must, within reason:

- Disclose misconduct discovered at the acquired entity **within six months** of date of closing and
- Fully remediate the conduct **within a year** from the date of closing

Safe Harbor Policy applies only to bona-fide, arms-length transactions

Mitigation: Diligence and Integration

U.S. enforcement authorities expect effective compliance programs to undertake a series of risk-based diligence and integration steps in the M&A context, both before and after an acquisition. Some key considerations are:

1. Communications and Training

Communicating clear expectations for personnel on “Day One” and during the integration period is a critical, threshold step to instilling a culture of compliance at the acquired business and to surfacing any legacy or ongoing risks

2. Risk Assessment

Leveraging and complementing the pre-acquisition diligence, a company (with their counsel) should conduct a compliance-focused risk assessment, with a goal of developing a risk profile that is particularized to the acquired business and that would form the basis for compliance enhancements

3. Third Parties

In light of the elevated corruption risks posed by third parties, developing a risk-based plan to diligence and integrate ongoing third-party relationships

Compliance Considerations

05

The Relevance of Corporate Compliance Programs

- Effective corporate compliance programs are an integral aspect of good governance.
- For a company that is subject to a regulatory or criminal investigation, however, a compliance program serves an additional purpose: To demonstrate that any violation occurred **in spite of** the company's best efforts to conduct its operations consistent with the law and to inculcate legal and regulatory compliance as a value among its directors, officers, employees, and agents.
- Prosecutors and regulators will credit a company for efforts to improve its compliance program that are taken both **before** and **during** an investigation.
 - This credit can be significant, especially when paired with cooperation with the government investigation and self-reporting of misconduct.
 - In certain cases, a company's compliance and cooperation can even result in the government declining to bring a case that it would otherwise charge.
- As a result, an effective compliance program is a key asset for any large company, particularly those that are publicly traded.

A Framework for OFAC Compliance Commitments



- OFAC expects organizations to “employ a **risk-based approach** to sanctions compliance.”
- In 2019, OFAC published “A Framework for OFAC Compliance Commitments,” identifying **five essential components** of a strong sanctions compliance program.
- Recent enforcement actions continue to highlight the importance of maintaining a strong sanctions compliance program, including procedures such as **screening third parties and transactions** to identify possible touchpoints to OFAC-sanctioned persons and jurisdictions.

A Framework for OFAC Compliance **Commitments**

Management Commitment	Risk Assessment	Internal Controls	Testing and Auditing	Training
<p>Senior management promotes a culture of compliance and:</p> <ul style="list-style-type: none"> • Has reviewed and approved the sanctions compliance program • Ensures compliance unit has sufficient resources, authority and autonomy and • Recognizes seriousness of apparent violations, and remediates appropriately 	<p>Holistic, risk-based assessment</p> <ul style="list-style-type: none"> • Designed to identify sanctions risks that a particular organization is likely to encounter • Informs policies, procedures, internal controls and training <p>Examines touchpoints to the outside world</p> <ul style="list-style-type: none"> • Customers, supply chain, intermediaries and counterparties • Products and services offered and • Geographic locations 	<p>Internal controls adequately address risks</p> <ul style="list-style-type: none"> • Establish processes to identify, interdict, escalate, report and keep records of transactions that implicate OFAC's prohibitions <p>Written policies and procedures</p> <ul style="list-style-type: none"> • Clearly communicated to relevant personnel <p>Technological solutions</p> <ul style="list-style-type: none"> • Selected and calibrated based on organization's risk profile and • Tested for effectiveness 	<p>Comprehensive, independent, and objective testing or audit function</p> <ul style="list-style-type: none"> • Accountable to senior management and • Adequate authority, skills and resources <p>Negative testing or auditing results lead to immediate and effective action to identify root cause and remediate</p>	<p>Periodic training for all relevant employees</p> <ul style="list-style-type: none"> • Provided at least annually • Conveys job-specific knowledge of OFAC sanctions and • Holds employees accountable through scored assessments <p>Further tailored to high-risk employees</p> <p>Easily accessible training resources</p>

AML Compliance Programs

Compliance program best practices:

- ✓ Under the BSA, financial institutions must maintain a risk-based, written AML program “reasonably designed” to prevent money laundering and terrorist financing and ensure compliance with applicable BSA requirements.
- ✓ Create an AML program based on ongoing business-specific risk assessment using an established methodology that considers customer base, geographies, and services.
- ✓ Employ a qualified BSA/AML officer with adequate experience, authority, and staff support.
- ✓ Create internal controls addressing every aspect of the program, including governance and compliance with specific legal requirements.
- ✓ Maintain adequate ongoing and tailored AML training and communication.
- ✓ Conduct independent testing by qualified internal or external auditors.
- ✓ Integrate elements of the FinCEN Culture of Compliance for Financial Institutions guidance into AML program.
- ✓ Regularly update risk assessment for AML program, including for new products, services, customer base, and geographic locations.

AML Compliance Programs (con't)

Compliance program best practices continued:

- ✓ Regulators do not require the use of any particular technology or system. While they support the use of innovative technology to increase the efficacy of the BSA/AML Programs, it is not uncommon for the exam team to scrutinize the use of such technology on the ground level.
- ✓ It is imperative that compliance programs grow and evolve alongside growth and changes in the business.
- ✓ Engage in ongoing oversight for counterparties, with monitoring of activity and compliance examinations at risk-based intervals.
- ✓ Consistent with the dollar thresholds establishing reporting requirements for senders and receivers, there should also be full compliance with the CTR, KYC, SAR and OFAC requirements.
- ✓ Comply with law enforcement requests and share information with other financial institutions.
- ✓ Utilize mechanisms for signal sharing amongst compliance teams, such as a “centralized clearinghouse” for information gleaned from law enforcement subpoenas and other signals and information that contribute to the success of the program.
- ✓ Integrate compliance involvement and review to assess risks during product development.
- ✓ Implement the three lines of defense model (business, compliance, and internal audit), as well as continual training and messaging on the culture of compliance.

DOJ Guidance and Precedent

Recent Guidance

During the Biden Administration, DOJ issued numerous updates to its corporate enforcement policies, as well as other pronouncements that are relevant to corporate compliance:

- **September 2022** – Memorandum from DAG Lisa Monaco, “Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group”
- **January 2023** – Remarks by Criminal Division Assistant AG Ken Polite, “Revisions to the Criminal Division’s Corporate Enforcement Policy”
- **March 2023** – DOJ Updates to Corporate Enforcement Programs, including Compensation Clawback Pilot Program
- **September 2024** – DOJ Updates to Corporate Enforcement Programs

DOJ Guidance and Precedent

September 2022 Policy Updates

On September 15, 2022, Deputy Attorney General Lisa Monaco issued a memorandum updating prior guidance concerning DOJ's corporate criminal enforcement priorities with the benefit of a year-long study by the Corporate Crime Advisory Group.

The announcement covered six key areas generally relevant to white collar corporate crime:

1. Placing a clear [priority on individual prosecutions](#);
2. Providing guidance on evaluating companies' [history of misconduct](#);
3. Requiring all corporate criminal enforcement components of DOJ to [develop voluntary self-disclosure policies](#);
4. Providing guidance on evaluating [corporate cooperation](#);
5. Providing guidance on evaluating [corporate compliance programs](#); and
6. Providing guidance on the [imposition of corporate compliance monitors](#).

The memorandum emphasized the importance of prosecutors' considering the [timeliness of companies' reporting](#) on individual misconduct and on companies' [engaging in compensation clawbacks](#) from executives and other [compensation disincentives](#) to shift the burden of financial penalties arising from enforcement.

DOJ Guidance and Precedent

January 2023 Policy Updates

On January 17, 2023, then-Criminal Division Assistant Attorney General Kenneth A. Polite, Jr. issued an updated [Criminal Division Corporate Enforcement & Voluntary Self-Disclosure Policy](#) that fulfilled DAG Monaco's instruction that each DOJ criminal enforcement unit adopt updated self-disclosure policies. The Criminal Division policy expanded on a prior policy that has applied to DOJ prosecution of FCPA matters since 2016.

The principal updates in the 2023 Policy are:

- [An increase to the maximum credit](#) a company can receive for cooperation, remediation, and/or voluntarily disclosure.
- [Enhanced guidance on the point within the Sentencing Guidelines range from which credit is applied](#) for cooperating, non-cooperating, and recidivist companies.

In February 2023, materially the same guidance was issued to all 93 U.S. Attorney's Offices around the country.

DOJ Guidance and Precedent

March 2023 Program Updates

In March 2023, DOJ issued a series of updates to its corporate compliance programs, including:

- Revisions to the [Evaluation of Corporate Compliance Programs](#)
- A [Revised Memorandum on Selection of Monitors in Criminal Division Matters](#) and
- A [Criminal Division Pilot Program Regarding Compensation Incentives and Clawbacks](#).

These updates:

- Standardize the “fundamental questions” that prosecutors should ask in [assessing corporate compliance programs](#) in an investigation, in making charging decisions, and in negotiating resolutions
- Establish credit for the [clawback or recoupment of compensation from employees responsible for misconduct, directly or through lack of supervision](#), in appropriate cases and
- Address appropriate [compliance policies and procedures related to the use of personal devices and communication platforms](#), including ephemeral messaging applications.

DOJ Guidance and Precedent

September 2024 Program Updates

On September 23, 2024, the acting head of the Criminal Division, Nicole Argentieri, announced revisions to the **Evaluation of Corporate Compliance Programs**, including:

- **Risk Assessment:** Procedures and assessment of new risk factors, including the use of new and **emerging technology** (e.g., AI); assessing compliance program's effectiveness
- **Improved Training and Communication:** Focus on continuous and tailored training, use of technology, and **gauging employee engagement**
- **Confidential Reporting Mechanisms:** Company promotion of reporting misconduct; whistleblower and anti-retaliation protections
- **M&A:** Risk assessment of migrating or combining systems; **post-transaction compliance oversight**
- **Compliance Resources:** Investment in compliance, and compliance personnel access to the relevant **data resources** for effective analysis

DOJ Guidance and Precedent

Evaluation of Corporate Compliance

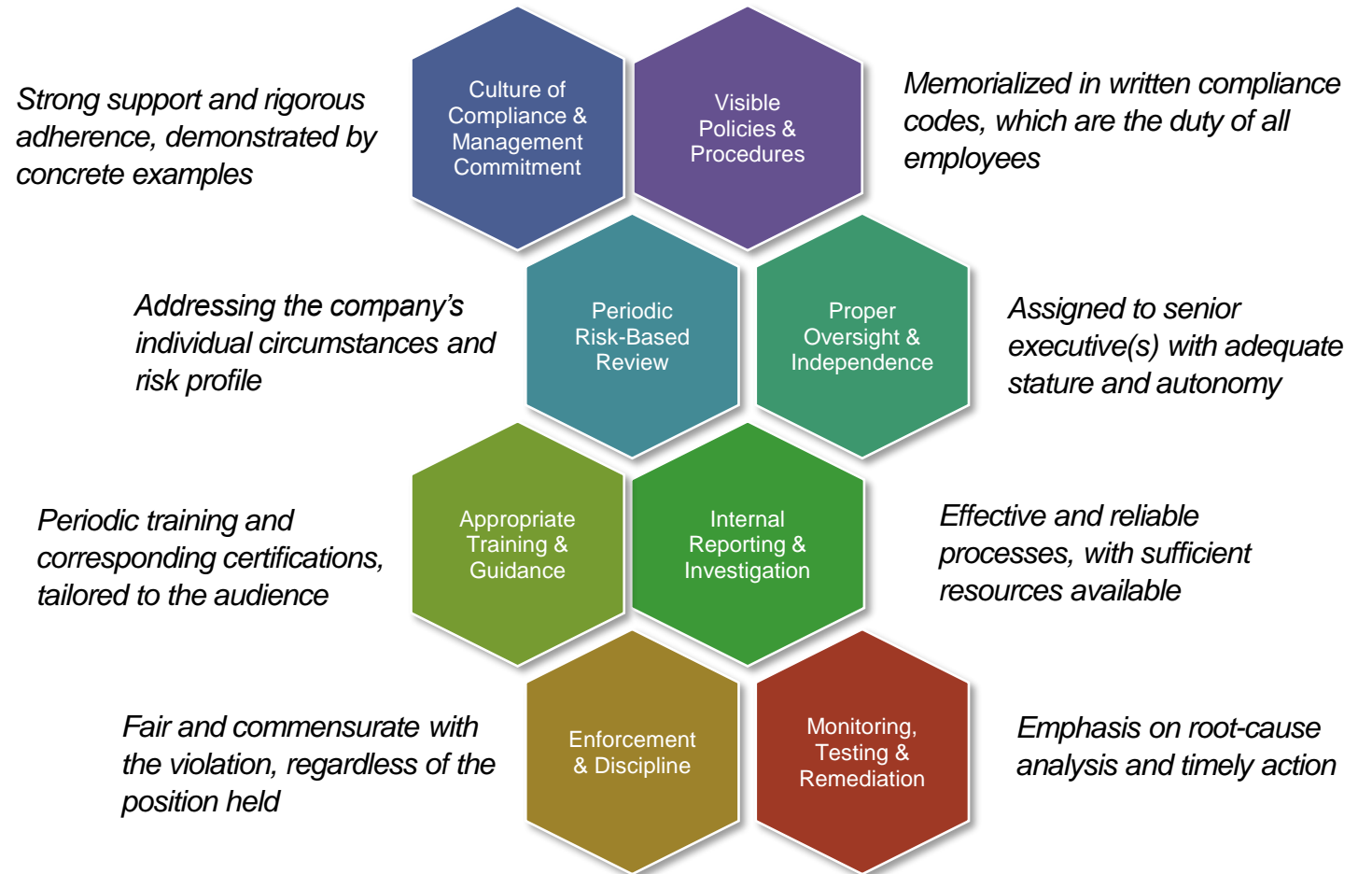
DOJ prosecutors are now directed to ask **three fundamental questions** about a corporation's compliance program:

- ✓ Is the corporation's compliance program **well designed**?
- ✓ Is the program **applied earnestly and in good faith**? In other words, is the program **adequately resourced and empowered to function effectively**?
- ✓ Does the corporation's compliance program **work in practice**?

DOJ Guidance and Precedent

Evaluation of Corporate Compliance (cont'd)

DOJ's Stricter Expectations for Corporate Compliance Programs



DOJ Guidance and Precedent

Evaluation of Corporate Compliance (cont'd)

- The Criminal Division now states that, subject to certain limitations, a company may be eligible for the [presumption of a declination](#) in a criminal investigation if it: (i) self-discloses the matter; (ii) fully cooperates; and (iii) timely and appropriately remediates.
 - There will be no declination if there are aggravating circumstances, such as recidivism or egregiousness.
 - If a prosecution occurs, DOJ will generally (i) recommend up to a [75% reduction off the low end](#) of the U.S.S.G. fine range (or off a higher point in the range for recidivists), (ii) not require a guilty plea, and (iii) not require a monitor.
- Additionally, in the M&A context, an acquiring company that identifies violations in pre- or post-acquisition due diligence can be eligible for a presumption of a declination if it self-discloses the conduct, cooperates with the investigation, and implements an improved compliance program at the acquired entity.
- Self-disclosure is a fact-specific determination and requires comprehensive consideration of all relevant factors because implementation of this and other DOJ policies varies from matter to matter.

DOJ Guidance and Precedent

Guidance on Comms. Policies

DOJ's new compliance guidance directs prosecutors to consider how companies maintain potential sources of discoverable communications outside of corporate systems.

In evaluating a company's compliance program, prosecutors are now directed to assess:

- The [types of communication channels](#) company personnel are permitted to use and use in practice;
- [Policies and procedures](#) governing employees' use of personal devices and communications platforms, including preservation of business communications; and
- The company's [risk management measures](#), including the consequences for employees' refusal to grant access to company communications.



DOJ's Whistleblower Policy and Pilot Program



In March 2024, Monaco announced the DOJ's new whistleblower program to incentivize individuals to come forward when they become aware of corporate wrongdoing.

- Under this policy, an individual who aids the DOJ in discovering “significant corporate or financial misconduct” of which the DOJ was previously unaware can “qualify to receive a portion of the resulting forfeiture” as a reward.
- DOJ will offer payments only to whistleblowers who:
 - Submit truthful information not already known to the government and
 - Are not involved in the criminal activity itself.
- Additionally, certain categories of whistleblowers, who would otherwise be at fault, could be offered non-prosecution agreements.

DOJ's Whistleblower Policy and Pilot Program



On August 1, 2024, DOJ released additional guidance on the pilot program, including the initial areas of focus:

- Filling important gaps in existing federal whistleblower programs.
- DOJ's pilot program is modeled on successful whistleblower programs run by the SEC, CFTC, and FinCEN, and seeks original information about corporate misconduct not covered by those programs.
- DOJ's program is focused initially on four areas: (1) certain crimes involving financial institutions and their employees; (2) foreign corruption involving privately held companies and others that are not issuers of U.S. securities; (3) domestic corruption involving companies; and (4) health care fraud schemes targeting private insurers not subject to qui tam recovery under the False Claims Act.

DOJ Guidance on M&A Diligence

In evaluating corporate compliance programs, the DOJ requires prosecutors to assess certain factors relating to a company's M&A practices:

- **Due Diligence Process** – Was the company able to complete pre-acquisition due diligence and, if not, why not? Was the misconduct or the risk of misconduct identified during due diligence? Who conducted the risk review for the acquired/merged entities and how was it done? What is the M&A due diligence process generally?
- **Integration in the M&A Process** – How has the compliance function been integrated into the merger, acquisition, and integration process?
- **Process Connecting Due Diligence to Implementation** – What has been the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process? What has been the company's process for implementing compliance policies and procedures, and conducting post-acquisition audits, at newly acquired entities?

In non-binding opinion releases, DOJ has recommended steps that an acquiring company can take to minimize exposure in the acquisition context:

- Conducting thorough risk-based FCPA and anti-corruption due diligence;
- Implementing the acquiring company's code of conduct and anti-corruption policies as quickly as practicable;
- Conducting FCPA and other relevant training for the acquired entity's directors and employees, as well as third-party agents and partners;
- Conducting an FCPA-focused audit of the acquired entity as quickly as practicable; and
- Disclosing any corrupt payments discovered through due diligence.

Sustainability and DE&I

06

Diversity – Regulatory Requirements

- **SEC requirements:** must disclose policy on diversity, how the board assesses its effectiveness and whether diversity was considered in the selection of a director
- **Nasdaq requirements:***
(no equivalent NYSE requirements)
 - **Board composition:** must have at least 1 female director & 1 director who is an underrepresented minority or LGBTQ+ or explain why not (subject to exceptions for smaller boards or companies)
 - **Disclosure:** matrix showing board-level data on gender diversity and race/ethnicity/LGBTQ+ diversity
 - ***Legal challenge:** In December 2024, the Fifth Circuit vacated the Nasdaq diversity rules, finding that the rules violated federal securities law and were not related to the primary purpose of the Securities and Exchange Act of 1934. Nasdaq announced that it will not appeal the ruling. The SEC has not announced its decision regarding a potential appeal.
- **Investor expectations:** often have specific numerical expectations on board diversity (see next slide)

Diversity – Investor Expectations

Institution	Gender	Race/Ethnicity
<i>Proxy Advisory Firms</i>		
ISS	1+	1+ (S&P 1500/Russell 3k)
Glass Lewis	30%+ (Russell 3000)	1+ (Russell 3000)
<i>Selected Institutional Investors</i>		
BlackRock	Case-by-case (S&P 500)	Case-by-case (S&P 500)
Vanguard*	Facts & circumstances based on sufficiency of progress	Facts & circumstances based on sufficiency of progress
Fidelity	2+ (10+ member boards)	1+
State Street*	30%+ (Russell 3k)	1+ (S&P 500/FTSE 100)
JPMorgan*	1+	1+

Investors may vote against the election of the nominating committee when these policies are not satisfied.






*Policies for 2025 not yet available for some of these investors.

SEC – Climate Rules

- **Background:** SEC adopted rules in March 2024, in a 3-2 vote along party lines.
- **Overview of required climate-related disclosures** in Form S-1 registration statement for IPO or annual report on Form 10-K:
 - **Governance:** board and management governance and practices for climate-related risk identification, assessment, management, and oversight, and related risk processes
 - **Risk:** climate risks with actual or potentially material impacts on financials, strategy, outlook and business model (but no need to disclose climate expertise on board)
 - **GHG emissions:** for larger companies, Scope 1 & 2 emissions, if material (but not Scope 3), with independent third-party assurance required on a phased-in basis
 - **Targets/goals:** climate-related targets or goals established by the company if materially or reasonably likely to materially affect financials, with annual progress updates
 - **Transition plans:** company-adopted transition plans, scenario analyses, and internal carbon pricing if used to assess material climate risks, plus related material expenditures
 - **Financial statement footnote:** reporting expenditures and costs of >1% due to “severe weather events,” “other natural conditions,” and certain carbon offsets and RECs
- **Legal challenge:** rules were challenged and stayed while subject to ongoing multi-district litigation in 8th Circuit.

Climate Change

– Investor Expectations

Institution*	
Proxy Advisory Firms	
	<ul style="list-style-type: none"> • TCFD-aligned disclosure for significant GHG emitters • Disclosure of GHG reduction targets
 GLASS LEWIS	<ul style="list-style-type: none"> • TCFD-aligned disclosure for S&P 500 in industries w/material GHG risk per SASB • Disclosure of climate-related risk mitigation and oversight
Selected Institutional Investors	
	<ul style="list-style-type: none"> • Recommends ISSB, IFRS S1 or S2-aligned disclosure
	<ul style="list-style-type: none"> • Suggests use of investor-aligned frameworks like ISSB
	<ul style="list-style-type: none"> • TCFD-aligned disclosure • Recommends disclosure of Scope 1/2 (and 3 if appropriate) GHG emissions & reduction targets • Enhanced disclosure for carbon-intensive industries

**Policies for 2025 not yet available for some of these investors.*

Other Climate Disclosure Rules

California

- **Background:** in October 2023, California adopted three wide-reaching bills that impose climate reporting requirements for public & private companies doing business or engaging in certain activities in CA.
 - **GHG emissions reporting:** annual disclosure of Scope 1, 2 & 3 emissions + 3rd party assurance (SB 253)
 - **Climate risk reporting:** biennial disclosure of climate risks and risk management (SB 261)
 - **Anti-greenwashing:** new disclosures for companies making certain sustainability claims (e.g., net zero, carbon neutral, significant emissions reductions) or deal in voluntary carbon offsets (AB 1305)
- **Who's in scope for SB 253/SB 261:** among others, companies organized under CA law or meeting sales, property or payroll thresholds in CA, with global annual revenues >\$1B (SB 253) or >\$500M (SB 261)
- **Legal Challenge:** rules were challenged in the CA Central District but have not been stayed.

Other Climate Disclosure Rules (cont'd)

European Union

- **Corporate Sustainability Reporting Directive (CSRD):** requires EU & non-EU enterprises with significant EU operations to report material environmental, social and governance matters (using a double materiality framework) in their annual report, including forward-looking, retrospective, qualitative and quantitative information
- **Corporate Sustainability Due Diligence Directive (CSDDD):** requires EU & non-EU enterprises with significant EU operations to identify and assess adverse human rights and environmental impacts, take steps to prevent/mitigate these impacts, and adopt a Paris Agreement-aligned climate change mitigation transition plan

Speaker Bios

07



Cynthia M. Mabry

Partner / [Houston](#)

811 Main Street, Suite 3000, Houston, TX 77002-6117

+1 346.718.6614

cmabry@gibsondunn.com

Cynthia Mabry is a partner in the Houston office of Gibson, Dunn & Crutcher. Cynthia concentrates her practice on capital markets, securities, mergers and acquisitions and general corporate matters. She represents public and private entities, investors and underwriters in capital markets and finance transactions, including offerings of equity and debt securities.

Cynthia also provides counsel on joint ventures, corporate governance and compliance matters. She is particularly experienced with clients engaged in the energy industry, including utilities, oil and gas exploration and production, midstream, oilfield services and other related sectors. Cynthia advises clients on governance structures and rapidly evolving legal and compliance issues related to climate change, environmental, social and corporate governance (ESG) and sustainability reporting. She frequently writes and speaks on topics relating to U.S. capital markets, climate change and sustainability.

Cynthia has been named among *Lawdragon's* 500 Leading U.S. Energy Lawyers 2023 - 2024, recognized by *Chambers Global* and *Chambers USA* for Capital Markets: Debt & Equity 2023 - 2024, Expert Guides *Rising Stars 2022 Guide* and named in *The Houston Business Journal* 2022 Women Who Mean Business List. *Texas Super Lawyers Magazine* has recently named Cynthia as a 2024 Super Lawyer for Securities & Corporate Finance.

Cynthia received her J.D. from The University of Houston Law Center in 2010. In 2004, she graduated from Louisiana State University with her Bachelor of Science in Accounting. Prior to practicing law, Cynthia worked as a senior associate at PriceWaterhouseCoopers in Houston.

Cynthia serves on the board of the University of Houston Law Foundation, and is Co-Chair of the University of Houston Law Center's Women of the Law. She is also a member of the advisory council to the Louisiana State University Ogden Honors College and the advisory council to the Tahirih Justice Center, Houston.

EDUCATION

[University of Houston](#)
Juris Doctor

[Louisiana State University](#)
Bachelor of Science



Adam M. Smith

Partner / [Washington, D.C.](#)

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

+1 202.887.3547

asmith@gibsondunn.com

Adam M. Smith is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher and serves as co-chair of the firm's International Trade Practice Group. He is an experienced international lawyer with a focus on international trade compliance and white collar investigations, including federal and state economic sanctions enforcement, CFIUS, the Foreign Corrupt Practices Act, embargoes, and export and import controls.

Chambers USA and *Chambers Global* consistently rank Adam as a leading attorney in International Trade: Export Controls & Economic Sanctions. In those publications, clients describe Adam as “a terrific resource for clients” and a “reassuring lawyer in a complex area of law.” Most recently, *Legal 500 US 2024* named Adam a “Leading Lawyer” in International trade: Customs, export controls and economic sanctions. *Global Investigations Review* has named him to its “25 Most Respected Sanctions Lawyers in Washington, D.C.” list, which features individuals who work on the most significant cases. *The Best Lawyers in America*® recognizes him for International Trade and Finance Law. *Who's Who Legal* regularly recognizes him as a Thought Leader for Trade & Customs, International Sanctions, and in its Global Elite Guide.

Clients benefit from Adam's experience in the Obama Administration, where he was Senior Advisor to the Director of the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and Director for Multilateral Affairs on the National Security Council. At OFAC, he was instrumental in shaping and enforcing sanctions policies, briefing Congressional and private sector leaders, conducting extensive international outreach, and negotiating complex agreements. On the National Security Council, he advised the President on international sanctions, coordinated inter-agency efforts, and developed strategies to counter corruption and promote asset recovery.

Adam is a 2006 *magna cum laude* graduate of Harvard Law School where he was a Chayes Fellow, the recipient of the Laylin Prize for the best work in international law, and the Senior Editor of the *Harvard International Law Journal*. He graduated *magna cum laude* from Brown University in 1996 with a Bachelor of Arts degree in Political Science and Economics, and an MPhil in Politics from Oxford University in 1998 where he was the Seaton Scholar in Politics at St. Hugh's College. Following law school, Adam served as a law clerk for the Honorable James Baker on the U.S. Court of Appeals for the Armed Forces.

EDUCATION

[Harvard University](#)
Juris Doctor

[University of Oxford](#)
Master of Philosophy

[Brown University](#)
Bachelor of Arts

CLERKSHIPS

[U.S. Court of Appeals, Armed Forces](#)

Patrick F. Stokes

Partner / [Washington, D.C.](#)

Patrick Stokes is a litigation partner in Gibson, Dunn & Crutcher's Washington, D.C. office. He is the co-chair of the Anti-Corruption and FCPA Practice Group and a member of the firm's White Collar Defense and Investigations, National Security, Securities Enforcement, Trials, and Litigation Practice Groups. Patrick's practice focuses on internal corporate investigations, government investigations, enforcement actions regarding corruption, securities fraud, and financial institutions fraud, and compliance reviews. He has tried more than 30 federal jury trials as first chair, including high-profile white-collar cases, and handled 16 appeals before the U.S. Court of Appeals for the Fourth Circuit. Patrick regularly represents companies and individuals before the DOJ and SEC, in court proceedings, and in confidential internal investigations. Patrick's experience covers every significant business sector and includes investigations, trials, and the assessment of corporate anti-corruption compliance programs and monitorships.

He is recognized by *Chambers Global* and *Chambers USA*, noting his "impressive government experience, having previously served as head of the FCPA unit at the DOJ" and that he "is regularly called on by corporations facing major investigations by the DOJ and SEC." He is also regularly recognized by *Benchmark Litigation*, *Global Investigations Review*, *Who's Who Legal Thought Leaders USA*, and *Best Lawyers in America*®.

Prior to joining Gibson Dunn, Patrick headed the FCPA Unit of the U.S. Department of Justice, where he managed the FCPA enforcement program and all criminal FCPA matters throughout the United States. Patrick also served as the DOJ's principal representative at the OECD Working Group on Bribery, working with law enforcement and policymakers from 41 signatory countries on anti-corruption enforcement policy issues. Patrick also served as Co-Chief of the DOJ's Securities and Financial Fraud Unit, overseeing investigations and prosecutions of financial fraud schemes involving corporations, financial institutions, and individuals. He also served as an Assistant United States Attorney in the Eastern District of Virginia, where he prosecuted a wide variety of financial fraud, immigration, and violent crime cases. Patrick received multiple awards while at the DOJ, including the Attorney General's Distinguished Service Award and the Assistant Attorney General's Exceptional Service Award (Criminal Division).

Patrick received his bachelor's degree and Juris Doctor from the University of Virginia, where he was an editorial board member of the *Virginia Journal of Social Policy and the Law*. He is a member of the Maryland State Bar and the District of Columbia Bar.



EDUCATION

[University of Virginia](#)
Juris Doctor

[University of Virginia](#)
Bachelor of Arts



Sam Raymond

Of Counsel / [New York](#)

200 Park Avenue, New York, NY 10166-0193

+1 212.351.2499

sraymond@gibsondunn.com

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.

Sam received his undergraduate degree from the Massachusetts Institute of Technology and his law degree from NYU Law School. Following law school, Sam clerked for Judge Mariana Pfaelzer of the Central District of California, and Judge J. Clifford Wallace of the United States Court of Appeals for the Ninth Circuit.

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](#)

GIBSON DUNN

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