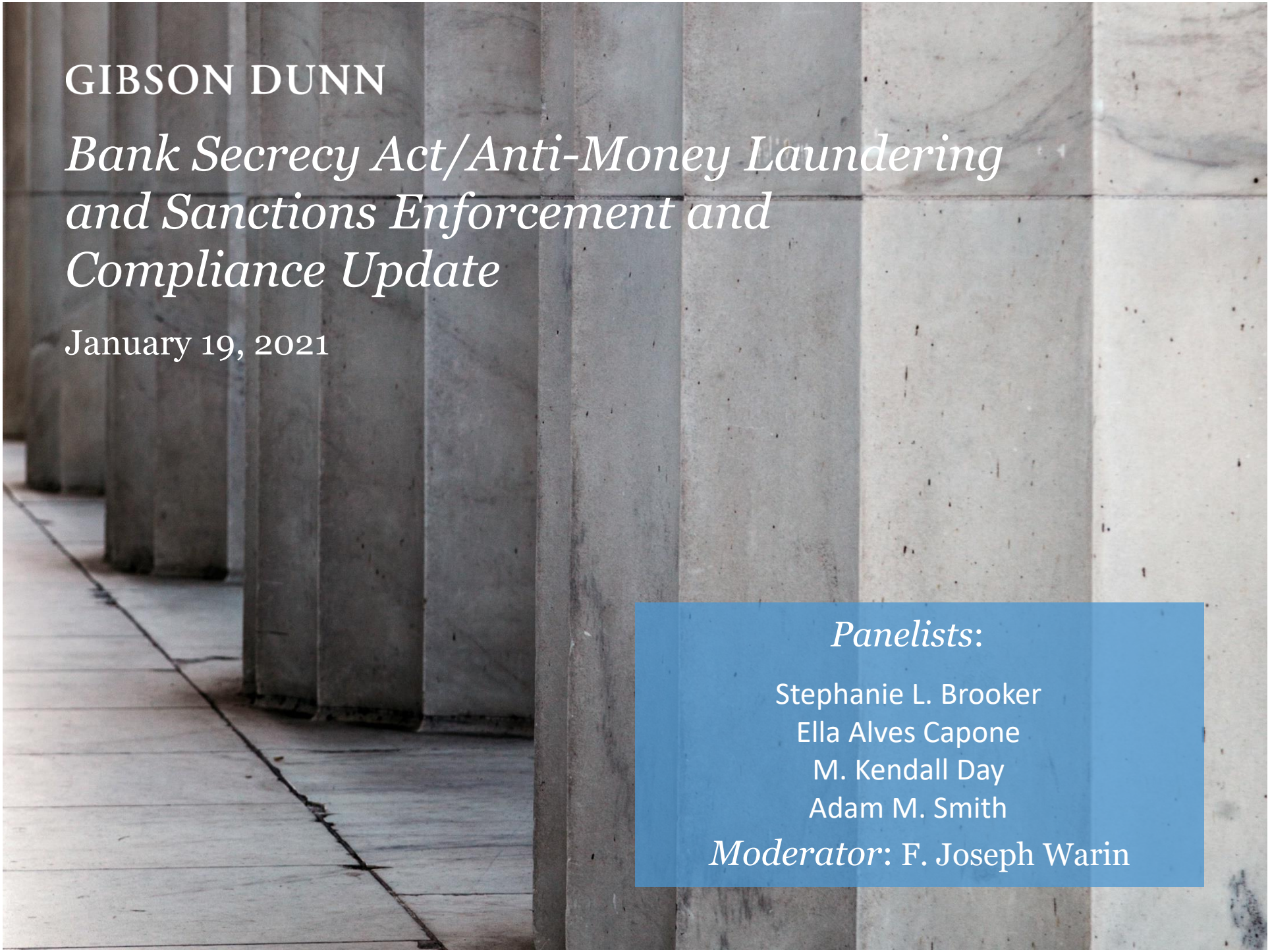


GIBSON DUNN

# *Bank Secrecy Act/Anti-Money Laundering and Sanctions Enforcement and Compliance Update*

January 19, 2021

*Panelists*:

Stephanie L. Brooker
Ella Alves Capone
M. Kendall Day
Adam M. Smith

*Moderator*: F. Joseph Warin

# MCLE Certificate Information

- Most participants should anticipate receiving their certificate of attendance approximately eight weeks following the webcast.
- All questions regarding MCLE Information should be directed to CLE@gibsondunn.com.

# Agenda

- **Introduction**
- **AML and Sanctions Under the Biden Administration**
- **Anti-Money Laundering Act of 2020**
- **U.S. Corruption Strategy and Focus on Gatekeepers**
- **Regulatory Guidance on Compliance Programs and Emerging Risks**
- **Cryptocurrency Guidance and Enforcement Actions**
- **BSA/AML and Sanctions Enforcement Actions**
- **Sports Betting and Online Gaming**
- **U.S. Measures Involving China**

GIBSON DUNN

# Introduction

# U.S. Enforcement Agencies and Regulators

## Enforcement Responsibilities

DOJ (Civil, Criminal, and Forfeiture)

SEC (Civil)

FinCEN (Civil)

CFTC (Civil)

OFAC (Civil)

FINRA (SRO)

## Bank Regulators and Enforcers

OCC

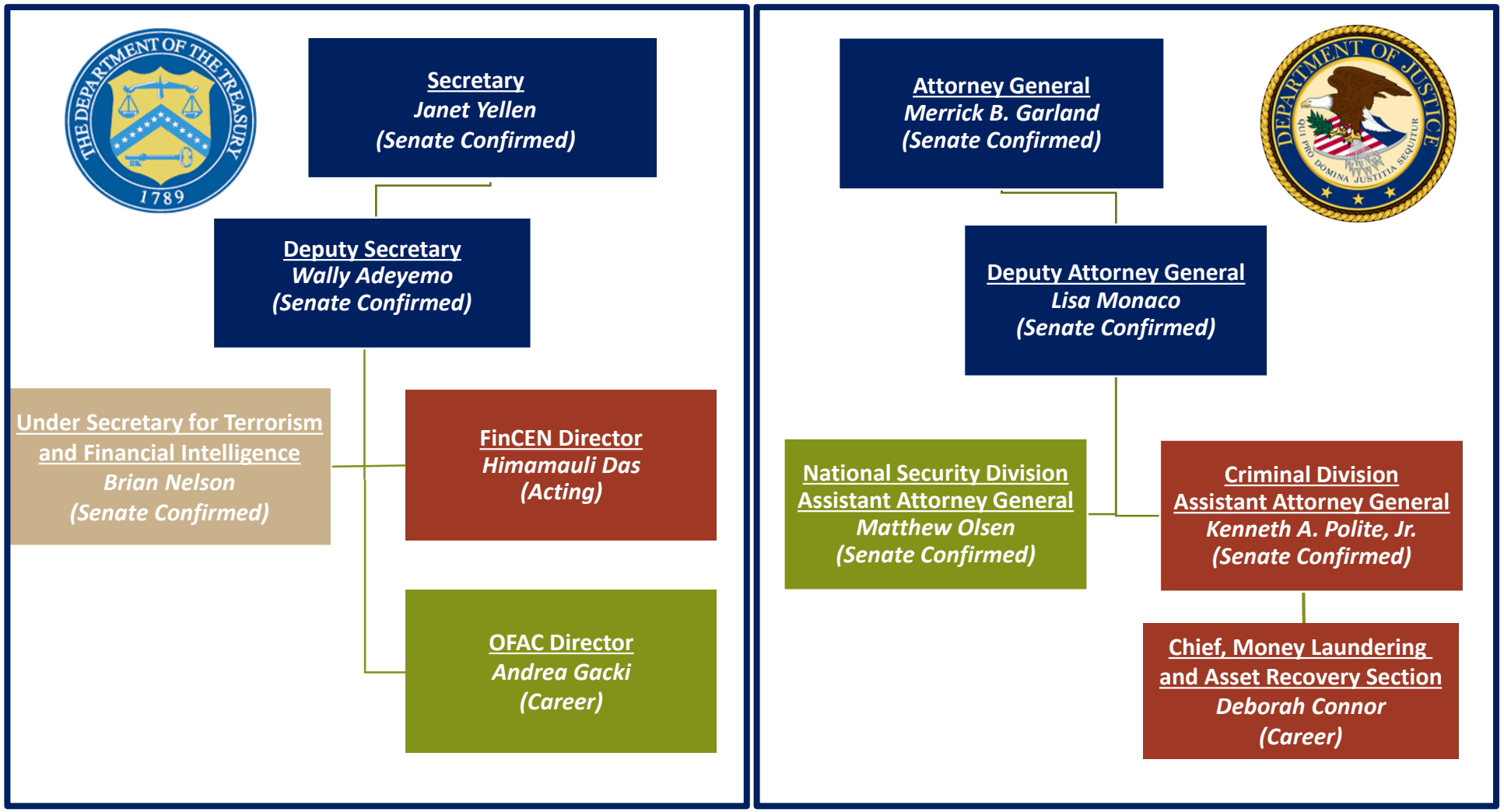
Fed

FDIC

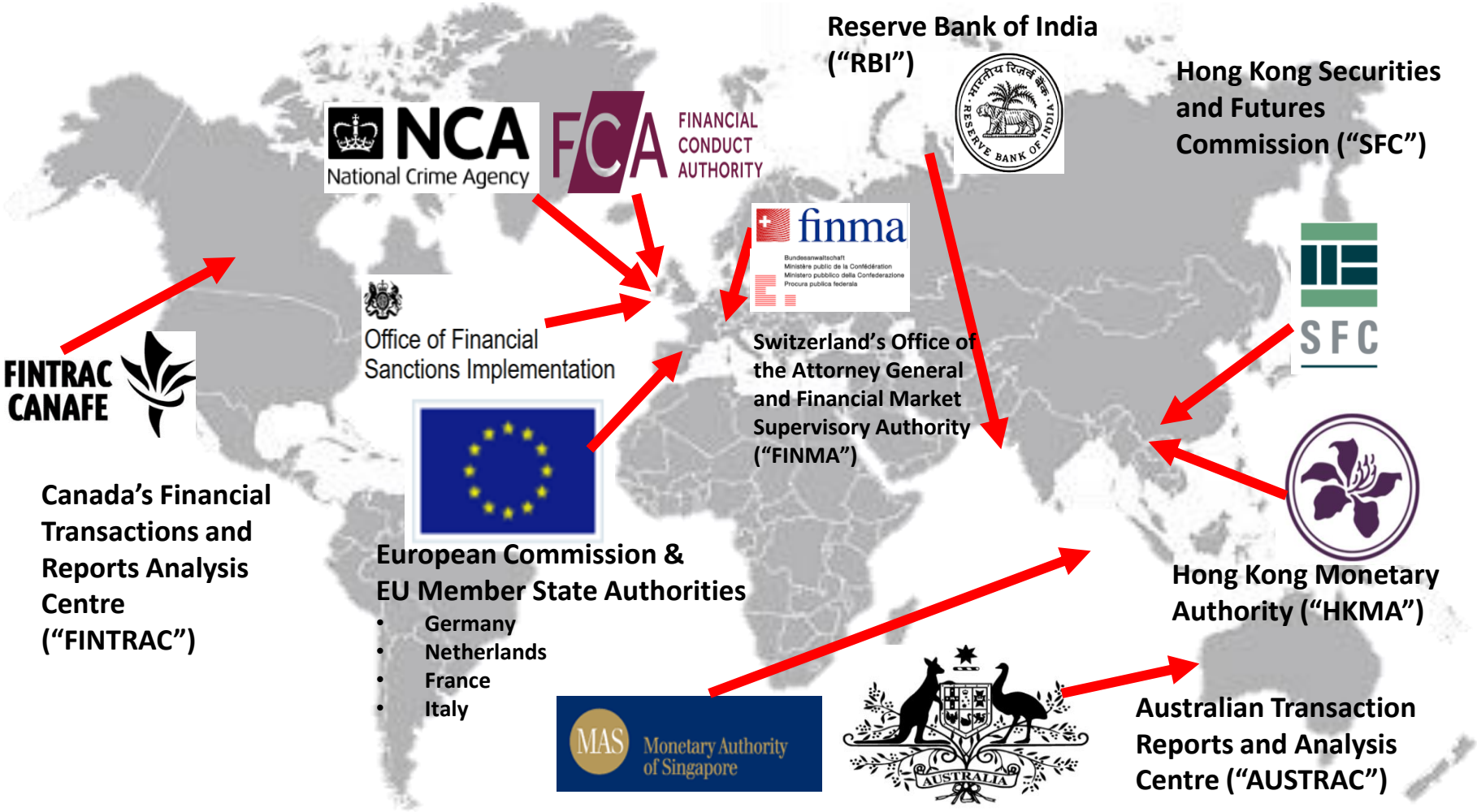
NCUA

DFS

# Treasury and DOJ Key Personnel



# International Enforcement Agencies and Regulators



# Types of U.S. Enforcement Actions

**Criminal:**

- Declinations
- Non-Prosecution Agreements
- Deferred Prosecution Agreements
- Guilty Pleas
- Trials
- Independent Monitors

**Resolutions May Include:**

- **Remedial Obligations**
- **Agreement to Forfeit Funds**
- **Criminal Fines**
- **Disgorgement**

**Regulatory:**

- **Informal Enforcement Actions**
- **Public Enforcement Actions**
  - Consent Orders, C&D Orders, Formal Agreements
- **Civil Enforcement Measures**
  - Civil Money Penalties
  - Remedial Measures, including SAR and CDD Lookbacks
  - Independent Monitors and Consultants
  - Extensive Regulatory Reporting and Oversight
  - Limitation of Business Lines and Growth

# AML Framework
## *Criminal Provisions - 18 U.S.C. 1956 and 1957*

- Under the anti-money laundering ("AML") statutes, **it is a crime to engage in a financial transaction with knowledge that the proceeds involved are the proceeds of unlawful activity if the government can prove that 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** – There are over 200 specified unlawful activities – U.S. and certain foreign crimes.
    - Foreign crimes: Bribery of a public official; misappropriation, theft, or embezzlement of foreign public funds; fraud, or any scheme or attempt to defraud, by or against a foreign bank; smuggling or export control violations; controlled substance violations; and specified violent crime offenses.
  - **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.

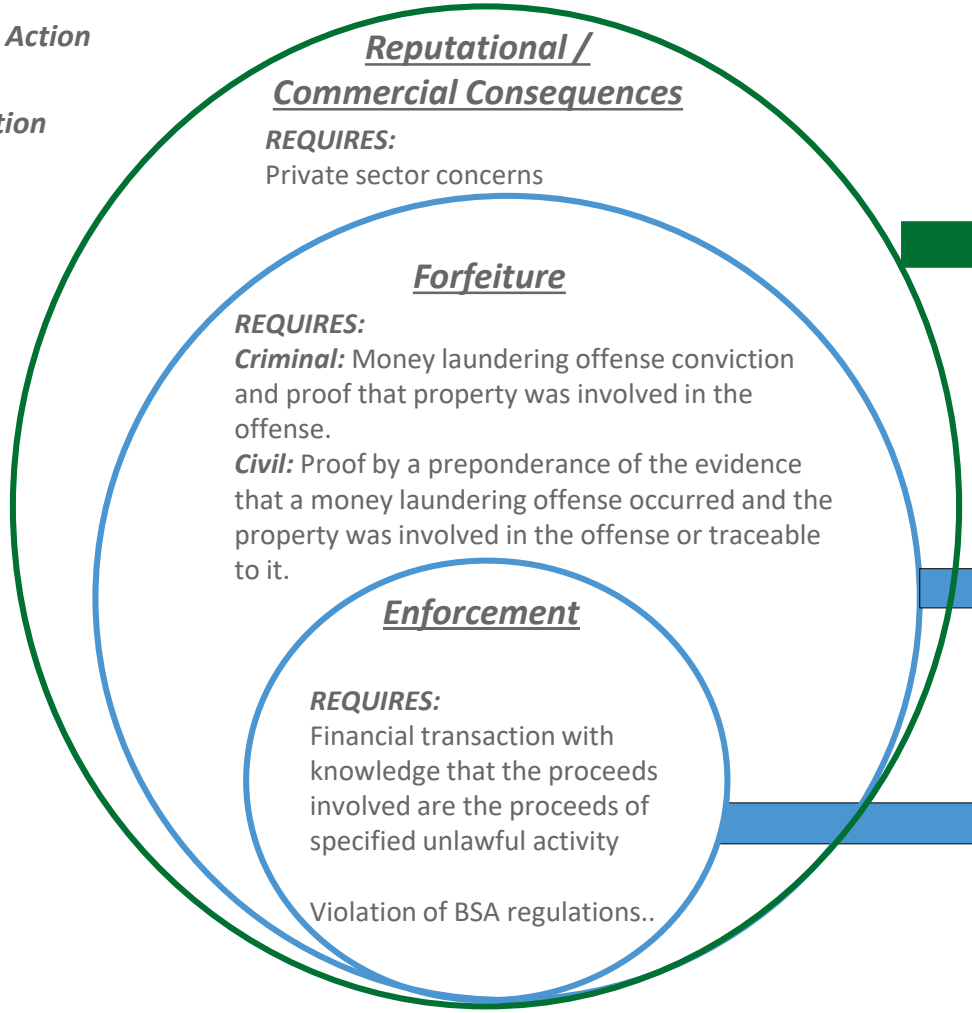
# AML Framework
## *The Bank Secrecy Act & Forfeiture*

- **The main source for AML reporting, recordkeeping, and compliance program regulatory requirements for "financial institutions" is the Bank Secrecy Act ("BSA"), 31 C.F.R. Chapter X**.
  - Unlike the AML criminal provisions, only certain businesses are subject to the BSA – banks, brokers or dealers in securities, money services businesses, telegraph companies, casinos and card clubs, futures commission merchants and introducing brokers in commodities, introducing brokers in commodities, mutual funds, insurance companies, dealers in precious metals, stones, or jewels, operators of credit card systems, loan or finance companies, and housing government sponsored enterprises.
  - Federal agencies can impose civil and criminal penalties for violations of the BSA. State banking agencies can impose similar penalties.
- **Funds involved in money laundering transactions or traceable to them can be subject to civil and criminal forfeiture**.
  - **Innocent owner defense.**

# AML Framework
## *Refresher on AML Risks*

***U.S. Government Action***

***Private Sector Action***




***Possible Outcomes***

- De-Risking
- Limited Transactions

- Loss of assets
- Financial impact

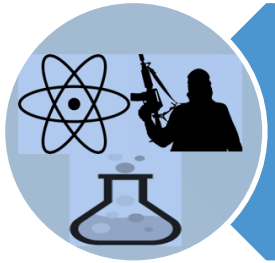
Civil and Criminal Consequences
- Potential Substantial Fines
- Potential Incarceration

# Sanctions Framework
*Primary v. Secondary*

## Primary Sanctions

### Jurisdiction-Based

Prohibit U.S. Persons from undertaking almost all transactions associated with a listed jurisdiction



### Behavior-Based

Prohibit U.S. Persons from undertaking almost all transactions related to entities listed for specific behaviors


### Sectoral Sanctions

Prohibit U.S. Persons from undertaking only limited, specific transactions with listed entities

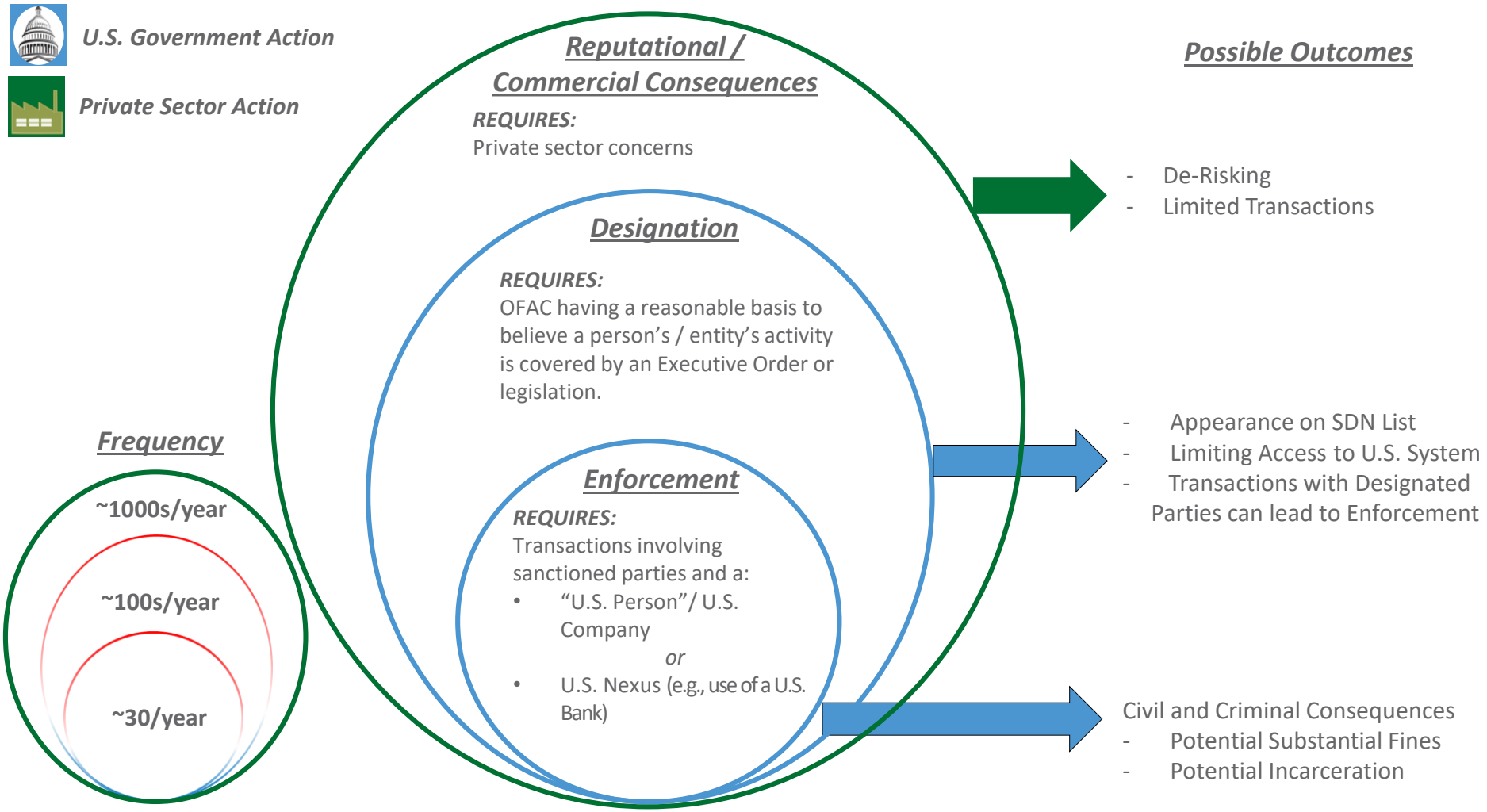
## Secondary Sanctions

### "With Us or Against Us"

Threaten the imposition of U.S. sanctions against non-U.S. persons for engaging in transactions with targeted entities

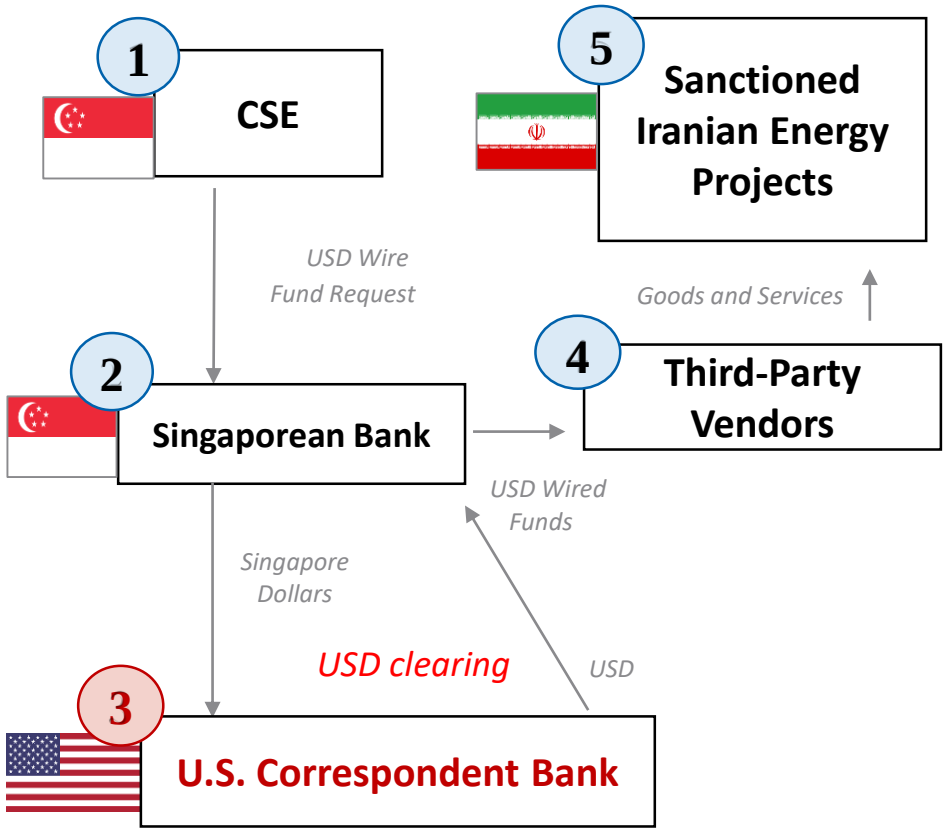
**In reality, *all* U.S. sanctions have become extraterritorial – some are just more extraterritorial than others**

# Sanctions Framework
## *Refresher on Sanctions Risks*



# Sanctions Framework
## *U.S. Dollar as Jurisdictional Hook*

- OFAC has targeted transactions conducted in USD even if the underlying transaction involves only non-U.S. entities. The "dollar clearing" process allows OFAC to claim U.S. jurisdiction.



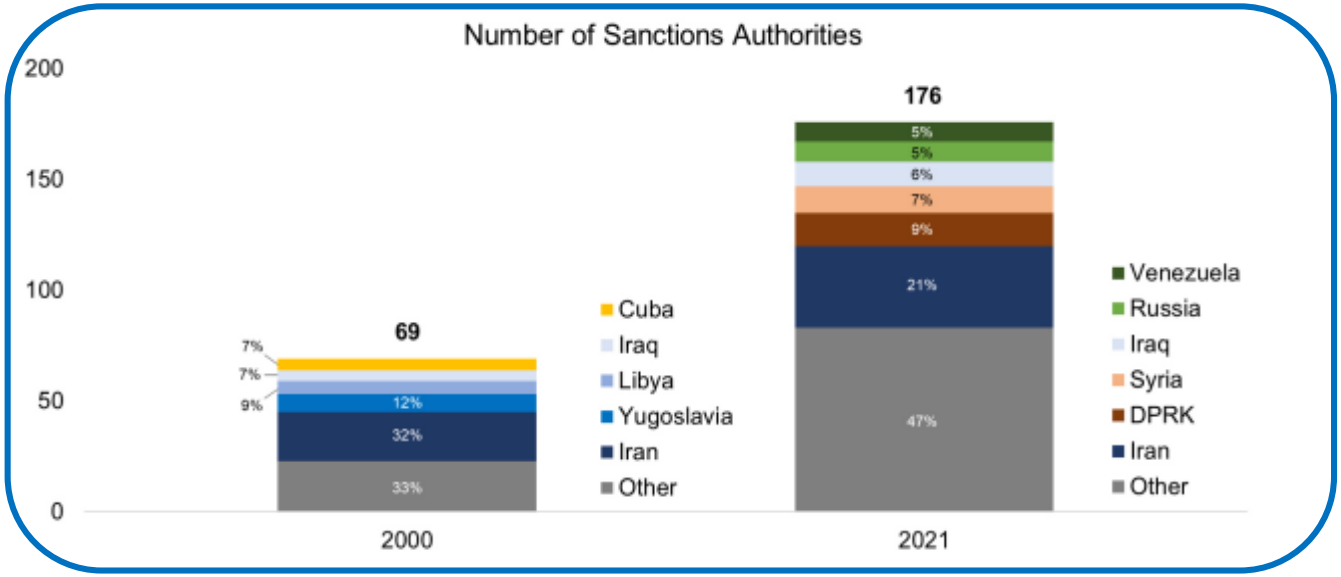

**In July 2017, CSE, a Singaporean telecom company, paid a $12 million penalty for "causing" U.S. financial institutions to violate U.S. sanctions against Iran.**

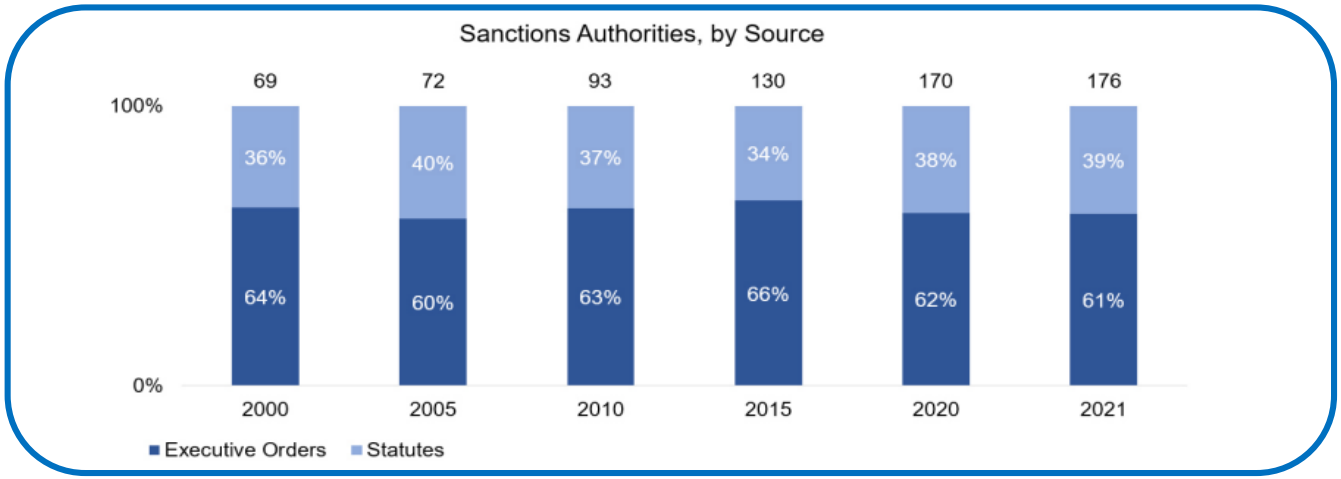
1. CSE agreed to provide goods and services to sanctioned Iranian energy projects.
2. CSE initiated 104 wire transfers in U.S. dollars from its Singaporean bank to third-party vendors providing goods and services on CSE's behalf for the sanctioned Iranian energy projects.
3. These wire transfers were "cleared" (i.e., converted) into U.S. dollars by the U.S.-based correspondent bank of the Singaporean bank.

*Because the wire transfers were in support of sanctioned Iranian projects, providing the dollar clearing service violated U.S. sanctions. Because CSE "caused" the U.S. correspondent bank to violate U.S. sanctions, CSE also violated U.S. sanctions.*

# Development of U.S. Sanctions Policy:
## *An Ever-Expanding Footprint for U.S. Sanctions*

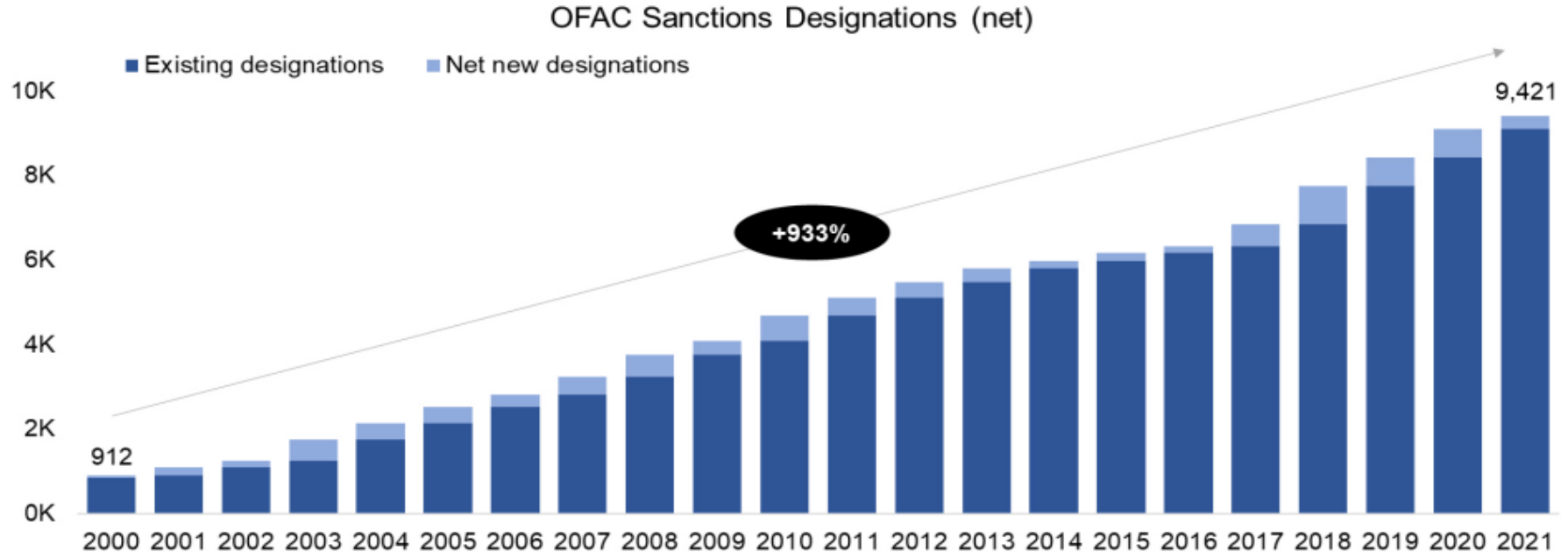
- On a bipartisan basis, the United States continues to rely on economic sanctions as a primary tool of diplomacy and national security.
- New programs have been instituted very quickly, blacklisted entities have been added and removed at an unprecedented pace, and the number and severity of enforcement actions—at both the federal and state levels—have increased remarkably.




Source: U.S. Dep't of Treasury, The Treasury 2021 Sanctions Review, Oct. 18, 2021.

# Development of U.S. Sanctions Policy:
## *An Ever-Expanding Footprint for U.S. Sanctions (cont'd)*




Source: U.S. Dep't of Treasury, The Treasury 2021 Sanctions Review, Oct. 18, 2021.

**92%↑**

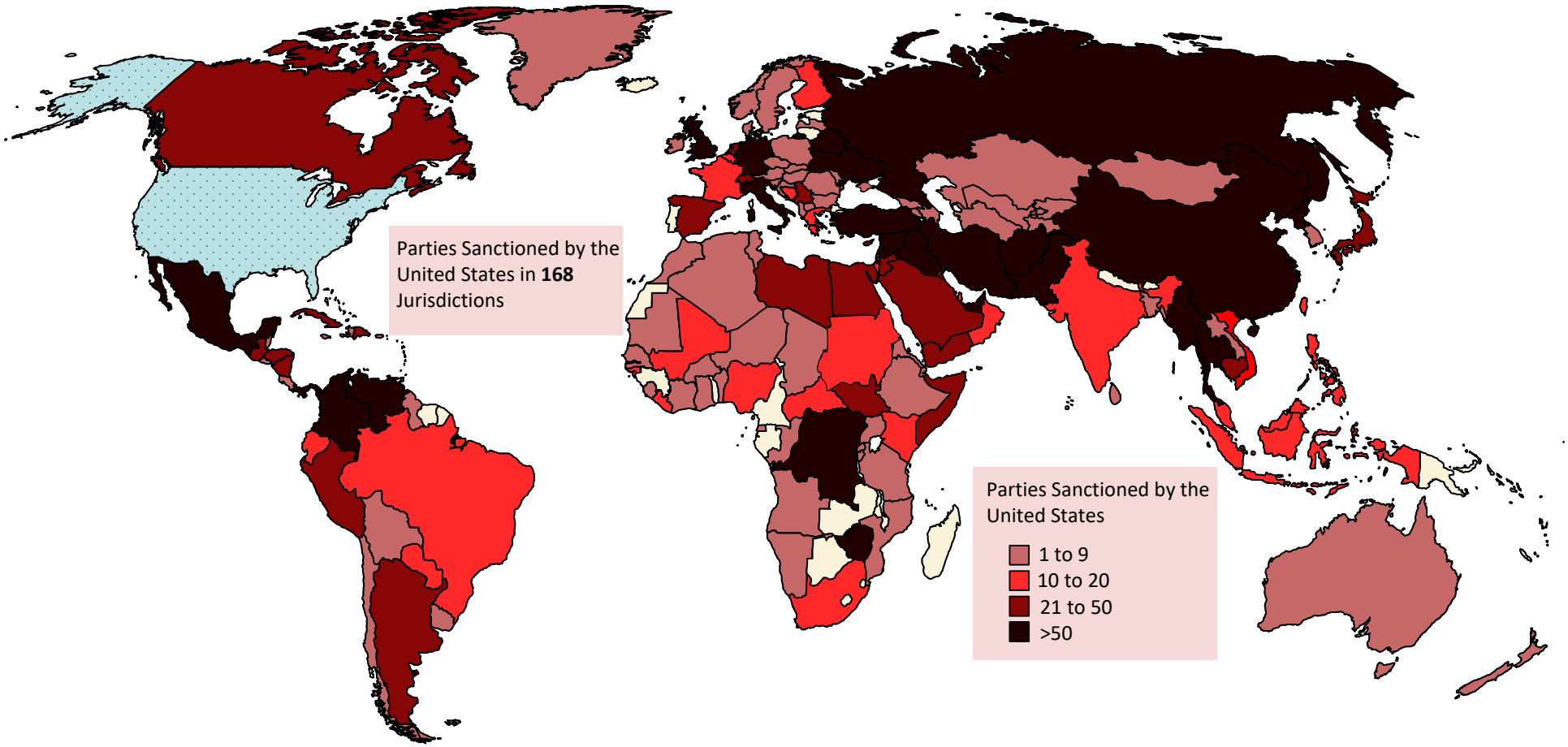
The increase in the number of individuals and entities on the SDN blacklist since 2010.

**>900**

Average annual additions to the SDN List from 2016 to 2020. This is nearly double the average from 2001 to 2015.

# Development of U.S. Sanctions Policy:
## *An Ever-Expanding Footprint for U.S. Sanctions (cont'd)*

**Distribution of parties designated as SDNs by the United States**



GIBSON DUNN

# AML and Sanctions Under the Biden Administration

# AML Modernization Initiatives

- One of FinCEN's overarching objectives in recent years has been to **modernize the BSA** to make its requirements more effective and efficient for today's financial industry, which has continued to be a primary focus under the Biden Administration.
  - A purpose of sweeping AML legislation passed on January 1, 2021 is "to modernize anti-money laundering and countering the financing of terrorism laws to adapt the government and private sector response to **new and emerging threats**."
- On December 14, 2021, FinCEN issued a **Request for Information seeking comments on ways to streamline, modernize, and update the AML/CFT regime** in the United States.
- Last week, FinCEN Acting Director, Himamauli Das, referenced the emerging "**transformation of the anti-money laundering/counter-terrorist financing regulatory regime *writ large***."

# AML Modernization Initiatives


"We recognize that the illicit finance threat landscape continues to evolve and that technology and innovation now play an important role in the efficient application of resources to combat illicit finance. I urge all relevant stakeholders to review the RFI and comment on ways that FinCEN can modernize AML/CFT regulations and guidance and better promote a risk-based approach to AML/CFT compliance."

Himamauli Das
FinCEN Acting Director

# AML Focus on Financial Innovation

- Consistent with the modernization initiative, Congress, FinCEN, and federal regulators have been focused on financial innovation, from **how emerging technology can be used to advance and modernize AML compliance and law enforcement efforts to how it poses unique risks.**
- Emerging topics in the spotlight include:
  - **Stablecoins;**
  - **Fintech relationships with community banks;**
  - **Cybersecurity and privacy;**
  - **Digital currencies; and**
  - **Ransomware.**

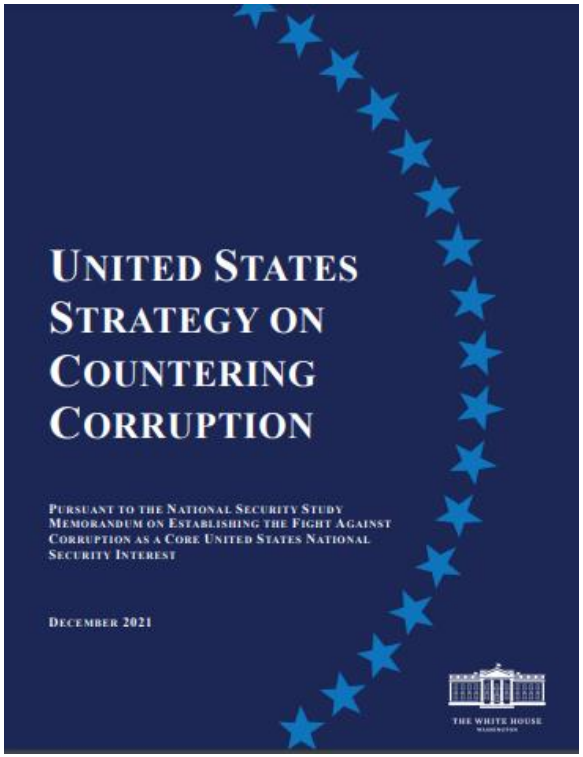
# AML Focus on Financial Innovation

"As the digital world increasingly becomes the financial world – and vice versa – we need a regulatory regime to match, one that accounts for crypto and other digital assets, evolution in the payments space, and other innovations that are driving the creation of new products, services, and delivery channels. FinCEN's view is that our regulatory framework needs to approach these innovations in a way that recognizes not only the risks that they pose, but the opportunities that they present."

Himamauli Das
FinCEN Acting Director

# AML Regime as a Tool to Combat Corruption

- On December 6, 2021, the Biden Administration released the **United States Strategy on Countering Corruption**, the first of its kind.
- Five "pillars" on which the Administration intends to build its anti-corruption efforts:
  1. **Modernizing, coordinating, and resourcing U.S. Government efforts to fight corruption;**
  2. **Curbing illicit finance;**
  3. Holding corrupt actors accountable;
  4. Preserving and strengthening the multilateral anti-corruption architecture; and
  5. Improving diplomatic engagement and leveraging foreign assistance to advance policy goals.
- The corruption strategy includes a significant focus on AML-related initiatives to combat corruption.



# Treasury's Sanctions Policy Review

- The Biden Administration is also re-evaluating the way the United States utilizes sanctions as a tool of foreign policy. In October 2021, the Treasury Department released a comprehensive Sanctions Review, outlining several principles to guide U.S. sanctions policy.
  - **Linking Sanctions to Clear Policy Objective** – Assess whether sanctions action is the right tool for the circumstances and whether it is part of a clearly-defined strategy.
  - **Multilateralism** – Coordinate with U.S. allies to magnify the economic and political impact of targeted sanctions.
  - **Avoiding Unintended Consequences** – Tailor sanctions to avoid economic, humanitarian, and political collateral damage to non-targeted populations.
  - **Communication** – Continue to engage with industry, financial institutions, allies, civil society, the media, and new constituencies.
  - **Investing in Sanctions Technology and Infrastructure** – Build technological capabilities and deepen institutional knowledge.

# Treasury's Stance on Sanctions Issues

- **The Biden Administration has expressed a desire to work with all key stakeholders to ensure maximum effectiveness of U.S. sanctions policy**

  - "This work requires close collaboration with Congress, across the executive branch, and with foreign counterparts, the private sector, and civil society... a carefully calibrated, strategic approach…is more important than ever,"

    *Elizabeth Rosenberg*
    *Assistant Secretary for Terrorist Financing*
    *Treasury Department*

  - The administration's approach to sanctions is meant to "ensure that sanctions remain an effective national security tool."

    *Adewale Adeyemo*
    *Deputy Secretary*
    *Treasury Department*

Source: https://www.wsj.com/articles/biden-to-temper-u-s-use-of-sanctions-weapons-officials-say-11625500717

GIBSON DUNN

# AML Act of 2020 Update and Associated Rulemaking

# AML Act of 2020 Update
*Overview*

- On January 1, 2021, Congress passed the **Anti-Money Laundering Act of 2020 ("AML Act of 2020")**, the most substantial and sweeping suite of legislative reforms to the U.S. AML and Counter-Terrorism Financing ("CFT") laws since the USA PATRIOT Act of 2001.
- The AML Act of 2020 generally addresses two primary objectives:

**Objective #1: Increasing BSA/AML Effectiveness and Modernization**

1. Beneficial ownership registry maintained by the U.S. Government [Sec. 6403]
2. Publication of AML Enforcement Priorities [Secs. 6101 and 6216]
3. Increased collaboration and feedback between Public and Private Sectors [Secs. 6203 and 6214]
4. Sharing of Suspicious Activity Reports (SARs) with foreign branches and affiliates [Sec. 6212]
5. CTR and SAR thresholds review and SAR streamlining [Secs. 6202, 6204 and 6205]

**Objective #2: Increasing BSA/AML Enforcement Authority and FinCEN Responsibilities**

1. Expanded subpoena authority for foreign bank records [Sec. 6308]
2. Expanded whistleblower provisions and BSA/AML penalties [Sec. 6314]

# AML Act of 2020 Update
## *Corporate Transparency Act*

- The AML Act of 2020 includes the Corporate Transparency Act ("CTA"), which implemented **beneficial ownership reporting requirements** for certain U.S. entities and foreign entities registered to do business in the United States ("reporting companies") and tasked FinCEN with **maintaining a beneficial ownership registry** of reported information.
  - A primary purpose is to combat money-laundering and terrorist financing through the use of shell companies.
  - Reporting companies must disclose **beneficial owners**, i.e., individuals who "exercise substantial control" over them or who own or control at least a 25% ownership interest.
  - There are a number of "reporting companies" exemptions, including for public companies, large companies, and many federally regulated companies.
  - The beneficial ownership registry will not be public. However, law enforcement will have access to it, and financial institutions with Customer Due Diligence requirements will be able to access the registry information with the reporting company's consent.
- FinCEN issued an **Advance Notice of Proposed Rulemaking in April 2021 and a Notice of Proposed Rulemaking in December 2021** to implement the beneficial ownership reporting provisions of the CTA.

# AML Act of 2020 Update
## *AML/CFT Priorities*

- The AML Act of 2020 requires FinCEN, in consultation with the Attorney General, federal and state financial regulators, and national security agencies, to publish **AML/CFT priorities**.
- On June 30, 2021, FinCEN published its first set of priorities:
  - Corruption
  - Cybercrime, including relevant cybersecurity and virtual currency considerations
  - Foreign and domestic terrorist financing
  - Fraud
  - Transnational criminal organization activity
  - Drug trafficking organization activity
  - Human trafficking and human smuggling
  - Proliferation financing
- Financial institutions will be required to "incorporat[e]" these priorities into their AML programs, which will be a measure "on which a financial institution is supervised and examined." The Unified Regulatory Agenda currently has FinCEN's Notice of Proposed Rulemaking for these regulations scheduled for April 2022.

# AML Act of 2020 Update

## *Increased Public-Private Collaboration and Feedback*

- The AML Act contains a number of provisions designed to further promote **collaboration between the public and private sectors**.
- It formalizes the FinCEN Exchange by statute and requires the Secretary of the Treasury to periodically report to Congress about the utility of the Exchange and recommendations for further improvements.
  - The **FinCEN Exchange** is FinCEN's voluntary public-private information sharing partnership among law enforcement, national security agencies, financial institutions, and FinCEN.
  - As part of the Exchange, FinCEN is authorized to furnish research, analytical, and informational services to financial institutions in the interest of detection, prevention, and prosecution of terrorism, organized crime, weapons proliferation, money laundering, and other financial crimes.
- The AML Act also requires the Secretary of the Treasury to convene a team consisting of stakeholders from the public and private sector "to examine strategies to increase cooperation between the public and private sectors for purposes of countering illicit finance."
- The AML Act also calls for feedback from law enforcement regarding the usefulness of SAR information filed by financial institutions.

# AML Act of 2020 Update

## *SAR Sharing with Foreign Branches and Affiliates*

- The AML Act of 2020 requires the creation of a **three-year pilot program** that allows a financial institution to share SARs and SAR information with the financial institution's foreign branches, subsidiaries, and affiliates, except those located in certain jurisdictions, including China and Russia.
  - The receiving institution must ensure that they do not disclose the SAR or share information contained in the SAR.
- This expansion of SAR sharing abilities has the potential to improve efficiencies in managing enterprise-wide risk, but may require some reconfigurations to case management systems and cybersecurity enhancements.
- The Unified Regulatory Agenda currently has a Notice of Proposed Rulemaking from FinCEN scheduled for March 2022.

# AML Act of 2020 Update

## *CTR and SAR Thresholds Review and SAR Streamlining*

- The AML Act requires the Secretary of the Treasury to "**establish streamlined, including automated, processes** to, as appropriate, permit the filing of noncomplex categories of reports."
- It also requires the government to conduct formal reviews of **whether CTR and SAR thresholds should be adjusted** and to determine if changes can be made to the filing process to "reduce any unnecessarily burdensome regulatory requirements" while maintaining a high degree of usefulness to law enforcement.
  - Current SAR and CTR thresholds were established over 20 and 50 years ago.
- Updates implemented as a result of these provisions may reduce the burden on financial institutions of adhering to outdated reporting threshold requirements and increase usefulness of information to regulators and law enforcement.

# AML Act of 2020 Update
## *Expanded Definitions - Antiquities*

- The AML Act **expanded the definition of "financial institution" to include a "person engaged in the trade of antiquities."**
- In September 2021, FinCEN issued an **Advance Notice of Proposed Rulemaking** seeking public comment on the nature of the antiquities business and compliance efforts as relevant to money laundering risks as well as proposed BSA regulatory applications to the industry.
- Based on the Unified Regulatory Agenda, FinCEN's Notice of Proposed Rulemaking is anticipated in June 2022.
- The AML Act also requires a study on the facilitation of money laundering and terror finance through the trade in works of art.

# AML Act of 2020 Update
## *Fintech Innovation Efforts*

- A major focus of FinCEN's BSA effectiveness review has been innovation in BSA compliance and prevention and detection of financial crime using modern technology, such as artificial intelligence.
- Congress directed FinCEN to carry on its **technology innovation efforts** with a number of very specific provisions in the AML Act, including:
  - Creation of a Subcommittee on Innovation and Technology in the BSA Working Group;
  - Appointment of an Innovation Officer at FinCEN;
  - BSA rulemaking on standards of testing for financial institutions applying new technology to BSA compliance;
  - Assessment of the impact of technology on financial crime and reporting with recommendations to Congress; and
  - Periodic technology symposiums.
- A cornerstone of FinCEN's technological innovation work has been its **Innovation Hours Program**, which was announced in May 2019. Since July 2019, FinCEN also has conducted monthly "Innovation Hours" meetings to discuss experiences and ideas for applying technology solutions to address financial crime, such as applying machine learning and artificial intelligence to identify suspicious activity, digital identification, and the facilitation of BSA compliance by virtual currency exchangers.
- In 2021, FinCEN held Innovation Hours on **privacy enhancing technologies** and announced a **Financial Crimes Tech Symposium**. On January 11, 2022, FinCEN and FDIC announced a **Digital Identity Tech Sprint.**

# AML Act of 2020 Update

## *Expanded Definitions - Cryptocurrency*

- The AML Act also added "value that substitutes for" currency, funds, and/or monetary instruments in BSA Statute definitions for financial agency, currency exchange, money transmitter, and monetary instrument, in order to explicitly cover virtual currency.
- The Act requires FinCEN to conduct a study into how virtual currencies and associated technologies are being used to further certain types of illicit conduct and methods for tracing virtual currency transactions.

# AML Act of 2020 Update

## *Expanded Subpoena Authority for Foreign Bank Records*

- The AML Act significantly expanded the scope of DOJ's and Treasury's authority to seek and enforce **correspondent account subpoenas** under 31 U.S.C. § 5318(k).
  - DOJ and Treasury are now allowed to seek "any records relating to the correspondent account or any account at the foreign bank, including records maintained outside of the United States," if the records are the subject of an investigation that relates to a violation of U.S. criminal laws, a violation of the BSA, a civil forfeiture action, or a Section 5318A investigation.
  - A foreign bank can petition a federal court to modify or quash the subpoena, but conflict with foreign confidentiality or bank secrecy law cannot be the sole basis for relief.
- The law includes a nondisclosure provision, meaning that the foreign bank is prohibited from notifying account holders involved, or any person named in the subpoena about the existence or contents thereof.
- The AML Act also contains **stronger enforcement mechanisms** – noncompliance can result in civil contempt and a civil penalty of up to $50,000 per day, as well as the loss of access to the correspondent account.

# AML Act of 2020 Update
## *Expanded Whistleblower Provisions*

- The AML Act significantly expands the **AML whistleblower award program**, providing that a whistleblower "shall" get an award of up to 30% of what was collected in AML enforcement actions resulting in monetary sanctions over $1 million.
  - In contrast, the prior program was discretionary and limited awards in most cases to $150,000.
  - Treasury has complete discretion to determine the amount of an award up to 30% with no minimum threshold.
- The law also includes broad **anti-retaliation protections** for whistleblowers.
  - This covers a broad range of disclosures, including not only ones made to federal regulatory or law enforcement agencies, but also internal disclosures to anyone with supervisory authority over the whistleblower or any other person working for the employer with authority to investigate, discover, or terminate misconduct.
- This may result in increases in internal and external whistleblower complaints, similar to what occurred when other whistleblower programs were similarly enacted or significantly expanded.
- The Unified Regulatory Agenda has a Notice of Proposed Rulemaking scheduled for April 2022.

# AML Act of 2020 Update
## *Expanded BSA/AML Penalties*

- The AML Act creates **two new offenses**:
  - Knowingly concealing or misrepresenting a material fact from or to a financial institution concerning the ownership or control of assets involved in transactions over $1 million involving assets of a senior foreign political figure or close family member or associate; and
  - Knowingly concealing or misrepresenting a material fact from or to a financial institution concerning the source of funds in a transaction involving an entity that is a primary money laundering concern.
- **Penalties** for violating these provisions are up to 10 years imprisonment and/or a $1 million fine.
- The Act additionally generally enhances penalties for various BSA/AML violations.

GIBSON DUNN

# U.S. Corruption Strategy and Focus on Gatekeepers

# U.S. Strategy on Countering Corruption

- The 2021 U.S. Strategy on Countering Corruption signals that the administration intends to push forward several long-standing potential gaps in the U.S. AML regulatory regime. In particular, its recommendations focus on:
  - Corporate Transparency
  - Investment Advisors
  - Dealers in Antiquities and Art
  - Other Gatekeepers – lawyers, accountants, and trust companies
- There have also been a series of corruption-related sanctions designations within the past several months.

# Focus on AML Regulatory Gaps for Gatekeepers

- In FATF's 2016 mutual examination, the U.S. was found to be noncompliant with several FATF recommendations due to an **AML regulatory gap for gatekeeper professions.**
- Some peer countries' AML regulatory regimes cover gatekeeper professions, some of which have been in existence for years.
- On December 6, 2021 FinCEN issued an **ANPRM for real estate transactions**, which states that "[l]awyers, accountants, and individuals in the private equity fields—all positions with minimal to no AML/CFT obligations under the BSA—often facilitate commercial real estate transactions."
- On December 23, GAO issued a report entitled Trafficking and Money Laundering: Strategies Used by Criminal Groups and Terrorists and Federal Efforts to Combat Them that highlights potential AML regulatory gaps related to gatekeepers.

# ENABLERS Act
## *Potential BSA Regulations for Gatekeepers*

**H. R. 5525**

- The **Establishing New Authorities for Business Laundering and Enabling Risks to Security Act ("ENABLERS Act")** was introduced in the House of Representatives by Rep. Malinowski on October 8, 2021.
- The proposed legislation would add "gatekeeper professions" (i.e. accountants, lawyers, art dealers, trust service providers, public relations businesses, and investment advisors) to the BSA's definition of "financial institutions."
- The ENABLERS Act would also **impose AML program and reporting requirements on all businesses defined as "financial institutions" by the BSA Statute, and remove FinCEN's ability to exempt businesses from such requirements**.
  - Currently, FinCEN has imposed AML Program, recordkeeping, and reporting regulatory requirements on most, but not all, of the businesses identified as financial institutions within the BSA.
    - For example, pawnbrokers, travel agencies, investment companies, and businesses engaged in vehicle sales are currently exempted from AML regulatory requirements.
- There is not currently a Senate version of the bill.

GIBSON DUNN

# Regulatory Guidance on Compliance Programs and Emerging Risks

# Compliance Programs and Emerging Risks
## *BSA/AML Programs*

- Financial institutions are required to maintain **risk-based BSA/AML Programs**.
  - Risk assessments should be updated with changes, as appropriate, to BSA/AML Programs when financial institutions change products, services, customers, or geographic locations.
- Although regulators do not require the use of any particular technology or system, they encourage (and expect) compliance programs to utilize innovative technology to increase the efficacy of BSA/AML Programs.
- In April 2021, **FinCEN, Federal Reserve, FDIC, OCC, and NCUA issued a Request For Information** about the extent to which the interagency Supervisory Guidance on Model Risk Management supports compliance by banks with BSA/AML and OFAC requirements to assess whether additional explanation or clarification may be needed.
- In March 2021, the **SEC issued a Risk Alert to broker-dealers**, observing that examiners have frequently discovered inadequate AML procedures and reporting systems and urging broker-dealers to strengthen their AML policies, procedures, and controls.
- In October 2021, **FINRA issued a regulatory notice** informing members of FinCEN's AML/CFT priorities and encouraging firms to incorporate those priorities into their AML/CFT programs.

# Compliance Programs and Emerging Risks
## *BSA/AML Outsourcing Trends and Guidance*

- Financial institutions are increasingly outsourcing portions of their BSA/AML compliance programs. Although outsourcing is permitted, it does not shift the financial institution's responsibility for BSA compliance.
  - Regulators have been focused on potential weaknesses to regulatory compliance and cybersecurity that may be introduced by outsourcing relationships.
- In July 2021, the Federal Reserve, FDIC, and OCC proposed interagency guidance on managing risk for third-party relationships, including with fintech partners.
- In August 2021, the Federal Reserve, FDIC, and OCC issued guidance to help community banks evaluate fintech relationships, given the increasing frequency of those relationships.
  - In September 2021, the Federal Reserve issued a report on Community Bank Access to Innovation through Partnerships that discusses different relationships between Community Banks and Fintechs and associated considerations and risks.
- In September, 2021, FINRA issued a regulatory notice that their Compliance Program vendors must meet its registration requirements.

# Compliance Programs and Emerging Risks
## *FinCEN Guidance Regarding Emerging Risks*

- FinCEN issued a few alerts in 2021 regarding upwards trends observed from SAR filings and other BSA data collected by FinCEN:
  - December 2021: **Wildlife trafficking**, which FinCEN noted as having a "strong association with corruption and transnational criminal organizations, two of FinCEN's national anti-money laundering and countering the financing of terrorism priorities…"
  - November 2021: **Environment crimes**, which FinCEN defined as including wildlife trafficking, illegal logging, illegal fishing, illegal mining, and waste and hazardous substances trafficking.
  - November 2021: **Ransomware and associated payments** through financial systems, most of which FinCEN noted involve CVC payments and attacks across governmental entities and financial, educational, and healthcare institutions.
  - September 2021: **Online child exploitation crimes**, which FinCEN noted increasingly involve CVC transactions, P2P mobile applications, the darknet, and anonymization and encryption services.
  - February 2021: **COVID-19 economic impact payments ("EIP") crimes**, which FinCEN flagged as including, in particular, fraudulent EIP checks, altered EIP checks, counterfeit EIP checks, theft of EIP from the mail, phising schemes using EIP as a lure, and inappropriate seizure of EIP.
  - February 2021: **COVID-19 health insurance and health care fraud**, including claims for unnecessary or false services, overbilling, kickbacks for services and testing, false representations about COVID-19 tests or treatments, telefraud schemes, and fraudulently obtaining COVID-19 health care relief funds.

# Compliance Programs and Emerging Risks
## *DOJ Focus on Cybercrime and Ransomware*

- DOJ has emphasized combatting cybercrime and ransomware as a top priority.

"A core priority of the Justice Department is to keep our country safe from all threats, foreign and domestic. Cybercrime is a serious threat to our country: to our personal safety, to the health of our economy and to our national security. Cybercrime takes many forms, one of which is ransomware. In ransomware attacks, transnational cybercriminals use malicious software to hold digital systems hostage and demand a ransom. These attacks have targeted our critical infrastructure, law enforcement agencies, hospitals, schools, municipalities and businesses of all sizes. Meeting this threat requires a whole-of-government approach. Together, with our partners, the Justice Department is sparing no resource to identify, and bring to justice, anyone, anywhere, who targets the United States with a ransomware attack."

- Attorney General Merrick B. Garland, November 8, 2021

"Today, one of the top priorities the Attorney General and I have is to make sure that we are best positioned and situated to deal with the cyber threat, as it rapidly evolves... Not a day goes by without ransomware headlines screaming at us from the newspapers. Earlier this year, the Department of Justice launched the Ransomware and Digital Extortion Task Force, to address this particular manifestation of the cyber threat…We are laser focused on investigating these cases and holding all those who help facilitate these crimes accountable — including, as I said, not only the attackers and the hackers and the affiliates who create and spread ransomware, but also the money launderers and the cryptocurrency companies that make it profitable."

- Deputy Attorney General Lisa O. Monaco, October 20, 2021

# Compliance Programs and Emerging Risks
## *DOJ Focus on Cybercrime and Ransomware*

- DOJ launched several initiatives in 2021 to combat cybercrime and ransomware:
  - **Ransomware and Digital Extortion Task Force**
  - **Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion**
  - **National Cryptocurrency Enforcement Team**
  - **StopRandomware.gov website**
  - **Civil Cyber-Fraud Initiative**
  - **Cyber Fellowship Program**
  - **Comprehensive Cyber Review**

# Compliance Programs and Emerging Risks
## *FinCEN Guidance on Ransomware and Cybercrime*

- FinCEN has likewise highlighted its focus on cybercrime and ransomware as increasing financial threats in its National BSA/AML Priorities and November 2021 Ransomware Alert.

> "Cybercrime is broadly defined as any illegal activity that involves a computer, another digital device, or a computer network. Cybercrime includes common cybersecurity threats like social engineering, software vulnerability exploits, and network attacks. Cybercrime is a significant illicit finance threat: the size, reach, speed, and accessibility of the U.S. financial system make covered institutions attractive targets to criminals, including terrorists and state actors…Treasury is particularly concerned about cyber-enabled financial crime, ransomware attacks, and the misuse of virtual assets that exploits and undermines their innovative potential, including through laundering of illicit proceeds."
>
> FinCEN National BSA/AML Priorities, June 30, 2021

# Compliance Programs and Emerging Risks
## *OFAC Guidance on Ransomware Payments*

- On September 21, OFAC issued an updated advisory warning of the sanctions risks of **facilitating ransomware payments** on behalf of cyber attack victims.
  - Ransomware is malicious software that blocks access to the victim's data.
  - Demands a ransom payment—often in the form of digital currency—to restore access.
- Sources of sanctions risk for **financial institutions** and **cyber insurance firms** include:
  - Growing number of malicious cyber actors are subject to U.S. sanctions.
  - Payments are frequently to anonymous recipients.
  - Challenging to assess whether funds are destined for an SDN or sanctioned jurisdiction.
- Should an apparent sanctions violation occur, OFAC will now take into account both the party's **cybersecurity practices** and whether the ransomware attack was **timely self-reported** to U.S. authorities in determining what enforcement response to impose.
- OFAC concurrently added SUEX OTC to the SDN List—the **first U.S. sanctions designation of a virtual currency exchange**—for facilitating ransomware payments.

*Photo source: Solarserven/iStock, via Getty Images Plus*

GIBSON DUNN

# Cryptocurrency Guidance and Enforcement Actions

# Cryptocurrency
## *FinCEN Focus*

- In May 2019, **FinCEN issued guidance** regarding the broad application of BSA registration, program, and reporting requirements to business models involving CVCs.
  - The AML Act's incorporation of language regarding value that substitutes for currency to several BSA Statute definitions reinforces this guidance.
  - Consistent with FinCEN guidance dating back to 2013.
- FinCEN included cryptocurrency as a **National AML/CFT Priority in 2021.**
- **DOJ's 2021 Cryptocurrency Enforcement Framework** highlights DOJ partnering with other agencies, including FinCEN and FATF, to prosecute cryptocurrency crimes and emphasizes how cryptocurrency-related businesses should maintain AML and sanctions compliance programs.
- FinCEN created a new position, **Chief Digital Currency Advisor** to the Director of FinCEN, which Michele Korver filled in July 2021.
- FinCEN has pending **reporting and recordkeeping** rulemaking that would require banks and MSBs to submit reports, keep records, and verify the identity of customers for transactions above certain thresholds that involve virtual currency wallets not hosted by a financial institution or hosted wallets in certain jurisdictions.
  - The Unified Regulatory Agenda has Final Action scheduled for September 2022.

*Photo source: OFAC*

# Cryptocurrency
## *FATF Guidance*

- In March 2021, the **Financial Action Task Force** issued updated guidance for **Virtual Assets ("VAs")** and **Virtual Asset Service Providers ("VASPs")**:
  - Expands the definition of what constitutes a VA and VASP and emphasizes that jurisdictions should not determine whether an entity is a VA or VASP based on the technology used or the label the entity applies to itself. Rather, the focus should be on the basic characteristics of the asset and/or service.
  - VAs "must be digital, and must themselves be digitally traded or transferred and be capable of being used for payment or investment purposes."
  - VASPs defined as any natural or legal person or business that conducts one or more of the following activities: (1) exchange between virtual assets and fiat currencies; (2) exchange between one or more forms of virtual assets; (3) transfer of virtual assets; (4) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; or (5) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

# Cryptocurrency
## *OFAC Guidance*

- On October 15, 2021, OFAC published industry-specific guidance tailored to the unique sanctions compliance risks faced by **virtual currency industry** participants, including technology companies, exchangers, administrators, miners, wallet providers, and users.
- Underscores OFAC's longstanding view that U.S. sanctions apply with equal force to transactions involving virtual and fiat currency.
- Offers a high-level primer on U.S. sanctions regulations and highlights sanctions compliance **best practices** that are especially relevant to virtual currency:
  - IP address geoblocking
  - Restricted party screening
  - Conducting "lookback" reviews after OFAC adds new virtual currency addresses to the SDN List


*Photo source: OFAC*

# Cryptocurrency
## *Treasury Guidance*

- In May 2021, the **Treasury Department** proposed a new reporting regime aimed at strengthening tax compliance, which is partially focused on cryptocurrency markets and transactions.
  - The proposed changes would create new reporting requirements built on the framework of existing 1099-INT forms that taxpayers currently use to report interest earned. Cryptocurrency exchanges and custodians would be required to report more information on the "gross inflows and outflows" of money moving through their accounts.
  - It also includes a requirement for transfers of at least $10,000 of cryptocurrency to be reported to the **IRS**.
  - Further, the report mentions that the proposal includes "additional resources for the **IRS** to address the growth of cryptoassets" and predicts that cryptocurrency is "likely to rise in importance."

# Cryptocurrency
## *FinCEN Enforcement Actions*

- In October 2020, the **Department of Justice** indicted the three founders and another employee of **BitMEX** alleging that they willfully failed to comply with BSA program compliance requirements. The **Commodity Futures Trading Commission** brought a companion civil enforcement action against five entities that conducted business as BitMEX and BitMEX's three founders.
  - In August 2021, **BitMEX** entered into resolutions with the **CFTC** and **FinCEN**, resulting in a total financial penalty of $80 million.
    - The **CFTC** consent order states that **BitMEX** failed to register as a futures commission merchant and failed to implement KYC, AML, and SAR programs. **BitMEX** is permanently enjoined from conducting business in the U.S. that involves the sale of cryptocurrencies or commodities.
    - **FinCEN**'s civil monetary penalty assessment states that **BitMEX** willingly failed to comply with its obligations under the BSA by failing to implement an AML program, hire compliance personnel, screen for VPN usage, implement a KYC program, and file SARs.

# Cryptocurrency
## *OFAC Enforcement Actions*

- In December 2020, **BitGo**, a cryptocurrency wallet management company, entered into a $98,000 settlement with **OFAC** to settle allegations that it violated multiple sanctions programs by processing cryptocurrency transactions for individuals located in Crimea, Cuba, Iran, Sudan, and Syria.
- In February 2021, OFAC announced a settlement of $507,375 with **BitPay, Inc. ("BitPay")** for allegedly facilitating approximately $129,000 worth of digital currency-related transactions for persons who appeared to be located in the **Crimea region, Cuba, North Korea, Iran, Sudan, and Syria**.
  - The settlement agreement specifically emphasizes that "OFAC obligations apply to all U.S. persons, including those **involved in providing digital currency services**."
  - While BitPay screened its direct customers (i.e., digital currency merchants), OFAC found fault with **BitPay's failure to screen location data the it obtained about the merchants' buyers** (i.e., the individual crypto currency purchasers).
  - OFAC believed that BitPay possessed sufficient information on those purchasers for screening purposes but did not perform the necessary screening.
- In March 2021, **Coinbase**, a centralized exchange, disclosed that certain of its transactions are "under review" by **OFAC** for potential violations of U.S. sanctions laws.

# Cryptocurrency
## *State Enforcement Actions*

- In February 2021, **New York Attorney General James** reached an agreement with **Bitfinex** and **Tether** to pay $18.5 million in penalties and cease doing business with persons in New York in connection with allegedly fraudulent representations about the financial reserves backing their products.
- In June 2021, **New York Attorney General James** also got a court order to shut down virtual currency trading platform **Coinseed** for operating without a license.
- And in July 2021, **Robinhood** announced it anticipates paying a $30 million fine to the **New York Department of Financial Services** in connection with anti-money laundering and cybersecurity issues at its cryptocurrency subsidiary.
- In September 2020, the **Massachusetts Attorney General** entered into a resolution with **Stripe** regarding allegations that it failed to conduct proper risk monitoring and fraud prevention in connection with a fraudulent initial coin offering.

GIBSON DUNN

# BSA/AML and Sanctions Enforcement Actions

# BSA/AML and Sanctions Enforcement Actions
## *OFAC*

- In recent years, OFAC has consistently brought enforcement actions against companies for sanctions violations resulting from the **failure of companies' automated screening systems** to detect transactions involving SDNs or other prohibited parties.
  - ***MoneyGram (April 2021)***: OFAC brought an action against MoneyGram Payment Systems, Inc. for allegedly providing services to blocked individuals incarcerated in U.S. federal prisons without a license from OFAC, processing transactions on behalf of a blocked person, and processing transactions for individuals who initiated commercial transactions involving Syria. OFAC cited MoneyGram's screening, technology, and fuzzy logic failures, as well as limited instances of human error, as the causes of these alleged deficiencies.
  - ***Payoneer (July 2021)****:* OFAC brought an action against Payoneer Inc. for allegedly processing payments for parties located in the Crimea region, Iran, Sudan, and Syria, and on behalf of SDNs due to deficiencies in its screening system, including weak algorithms, improper monitoring of IP addresses, failure to screen Business Identifier Codes ("BICs"), and insufficient focus on sanctions regions in screening.
  - ***TD Bank (December 2021)***: OFAC brought two actions against TD Bank, N.A for allegedly (1) processing transactions and maintaining accounts for 9 employees of the North Korean mission to the UN without a license, and (2) opening an account for an SDN. These situations resulted from screening deficiencies and accepting account applications with key information missing.

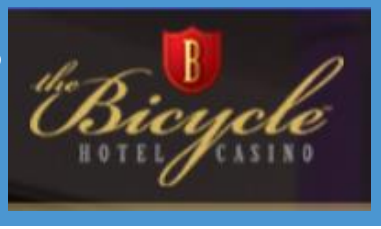
# BSA/AML and Sanctions Enforcement Actions
## *OFAC*

- On April 29, OFAC announced a settlement of $2,132,174 with **SAP SE ("SAP")** for 190 apparent violations involving the export of software and related services from the United States to Iran
  - Specifically, OFAC took issue with (1) SAP sending software to **companies in third countries** with knowledge or reason to know the software or services were intended specifically for Iran, and (2) the sale of **cloud-based software subscription services accessed remotely through SAP's cloud businesses** in the United States to customers that made the services available to their employees in Iran.
- OFAC cited the following **failures** in SAP's compliance function: (1) failure to **screen customers' Internet Protocol (IP) addresses** before permitting software downloads; (2) failure to fully **implement geo-blocking** based on IP addresses; (3) failure to conduct **sufficient due diligence on partners**; and (4) failure to **"timely integrate" acquired companies** into SAP's broader compliance structure.
- OFAC's actions emphasize a growing expectation that software providers (include cloud-based SaaS providers) properly **implement IP blocking and customer screening mechanisms**. Additionally, while not providing a specific timeline, OFAC is flagging the importance of conducting sufficient **pre- and post-acquisition due diligence** of compliance deficiencies in any M&A transaction and the **swiftly remediating such deficiencies** post-closing.

# BSA/AML and Sanctions Enforcement Actions
## *OFAC*

- On Jan. 3, 2022, **AirBnB Payments, Inc. ("AirBnB")** entered into a **settlement agreement** with OFAC to resolve allegations regarding transactions in violation of the Cuban Assets Control Regulations ("CACR").
- **Allegations:** From Sept. 2015 to Mar. 2020, AirBnB, through its subsidiary, allegedly:
  - Processed **3,464** "Stay" transactions for "Guests" traveling for reasons outside of OFAC's 12 authorized categories and processed **44** transactions involving non-U.S. persons prior to OFAC issuing a specific license to engage in such conduct; Processed **3,076** payments for "Experiences" without records documenting the provision of the CACR that authorized travel.
- **Penalty: $91,172.29**
  - OFAC accepted AirBnB's extrapolation from a "statistically significant sampling" of transactions to calculate the number of apparent violations and the average transaction amount for each violation.
  - The statutory maximum penalty was over $600 million; the base civil monetary penalty was $364,689.
  - OFAC credited AirBnB for its proactive steps to identify sanctions compliance issues, voluntary self-disclosure, and substantial cooperation during the investigation, and also considered that the violations were "non-egregious."
  - AirBnB agreed to "significant remedial measures," including an IP-blocking regime to account for technological issues that permitted violations, manual checks to ensure that no listings are associated with the Cuba Restricted List, and additional record-keeping and documentation practices.

# BSA/AML and Sanctions Enforcement Actions
*DOJ*




- On October 22, 2021, **The Bicycle Casino, L.P. ("Bicycle")**, a California-based hotel and casino, entered into a **two-year NPA** with the Central District of California to resolve an investigation into alleged violations of the BSA.
- **Allegations:** Bicycle allegedly failed to properly file CTRs and SARs, after a "high roller" Chinese national conducted millions of dollars in cash transactions at the casino in 2016.
- **Penalty: $500,000**
  - The penalty represents the revenue that Bicycle allegedly made from the foreign national in question.
  - Bicycle agreed to undergo enhanced review and reporting requirements to assure BSA compliance, including an audit by a third party and regular reporting to the U.S. Attorney's Office.
  - DOJ considered Bicycle's remedial efforts to strengthen its anti-money laundering program, as well as its cooperation with authorities during the investigation.

# BSA/AML and Sanctions Enforcement Actions
## *DOJ and SEC*


- On Oct. 19, 2021, **Credit Suisse Group, AG ("Credit Suisse")** entered into a **three-year DPA** with DOJ's MLARS and Fraud Sections and EDNY to resolve allegations that it engaged in conspiracy to commit wire fraud.
- **Allegations:** Credit Suisse, through its subsidiary, allegedly defrauded investors in connection with a Mozambique lending project. Credit Suisse allegedly hid information regarding the risk that proceedings from loans to three Mozambican government-owned entities were used to pay approximately $150 million in bribes to senior government officials and $50 million in kickbacks to two CSSEL employees.
- **Penalty: $247.5 million**
  - DOJ credited Credit Suisse for payments made to the SEC and United Kingdom's Financial Conduct Authority ("FCA"), under separate agreements with those agencies, including:
    - a $65 million civil penalty and $34.1 million in disgorgement and prejudgment interest to the SEC, and
    - a $200.6 million penalty to the FCA and a promise to irrevocably undertake $200 million of debt relief to Mozambique.
  - Credit Suisse did not receive either voluntary disclosure or full cooperation credit.

# BSA/AML and Sanctions Enforcement Actions
## *FinCEN*

- On January 15, 2021, **Capital One, National Association (Capital One)** consented to the assessment of a civil monetary penalty by FinCEN for alleged willful and negligent violations of the BSA and its implementing regulations.
- **Allegations:** From at least 2008 through 2014, Capital One allegedly:
  - Did not implement and maintain an effective AML program
  - Did not file thousands of SARS and CTRs related to the Check Cashing Group business, causing millions of dollars in suspicious transactions to go unreported, including proceeds connected to organized crime, tax evasion, fraud, and other financial crimes laundered through the bank into the U.S. financial system.
- **Penalty: $39 million**
  - FinCEN considered Capital One's significant remediation and cooperation with FinCEN's investigation.
  - In addition to exiting the Check Cashing Group and taking specific remedial efforts related to its SAR and CTR filing systems, Capital One made significant investments in and improvements to its AML program.
  - The bank also provided FinCEN with voluminous and well-organized documents, made several presentations of its findings, and signed several agreements tolling the statute of limitations during this investigation.

# BSA/AML and Sanctions Enforcement Actions
## *FinCEN and OCC*

- On December 16, 2021, FinCEN entered into a consent order with the **CommunityBank of Texas, N.A. ("CBOT")** for alleged willful violations of the BSA and its implementing regulations.
- **Allegations:** From at least 2015 through 2019, CBOT allegedly:
  - Did not implement and maintain an effective AML program
  - Did not report hundreds of suspicious transactions connected to tax evasion, illegal gambling, money laundering, and other financial crimes, even after the bank became aware that certain customers were subjects of criminal investigations.
- **Penalty: $8 million total**
  - $7 million FinCEN penalty.
  - In a coordinated settlement, OCC assessed a civil penalty of $1 million for BSA violations. FinCEN agreed to credit the $1 million civil penalty imposed by OCC.

# BSA/AML and Sanctions Enforcement Actions
## *Federal Functional Regulators*

- In November 2021, **Mashreqbank** entered into a global settlement with **OFAC, NYDFS, and the Federal Reserve** in connection with payments Mashreqbank's London branch processed through financial institutions in the U.S. between 2005 and 2009, in violation of now-repealed Sudanese Sanctions Regulations.
  - OFAC issued a Finding of Violation in lieu of a civil monetary penalty; Federal Reserve issued a Cease and Desist Order; NYDFS reached a Consent Order with a $100 million penalty.
- In October 2021, the **OCC** reached an agreement with **The Federal Savings Bank, Chicago, Illinois** based on unsafe or unsound practices related to the Bank's BSA compliance.
- In May 2021, the **SEC** announced settled charges against **GWFS Equities**, a broker-dealer, for alleged SAR violations. The agreement entailed a $1.5 million penalty.

# BSA/AML and Sanctions Enforcement Actions
## *FINRA*

- **Intesa Sanpaolo IMI Securities Corp. (December 2021)** – Letter of Acceptance, Waiver, and Consent for alleged AML Program deficiencies related to detecting suspicious activity involving low-priced securities transactions and diligence procedures for foreign financial institutions. Censure and $650,000 fine.
- **Luis Fernando Restrepo (July 2021)** – Letter of Acceptance, Waiver, and Consent for role as AMLCO in allegedly failing to implement a sufficient AML program and CIP.
- **Precision Securities LLC (July 2021)** – Letter of Acceptance, Waiver, and Consent for allegedly deficient AML Program. Censure and $350,000 fine.
- **Robinhood Financial (June 2021)** - Letter of Acceptance, Waiver, and Consent for, among other things, alleged CIP deficiencies. Censure, $57 million fine, restitution, and undertakings.
- **Score Priority Corp (April 2021)** - Letter of Acceptance, Waiver, and Consent for alleged AML Program deficiencies including relating to CIP and foreign financial institutions. Censure, $250,000 fine, and independent consultant.

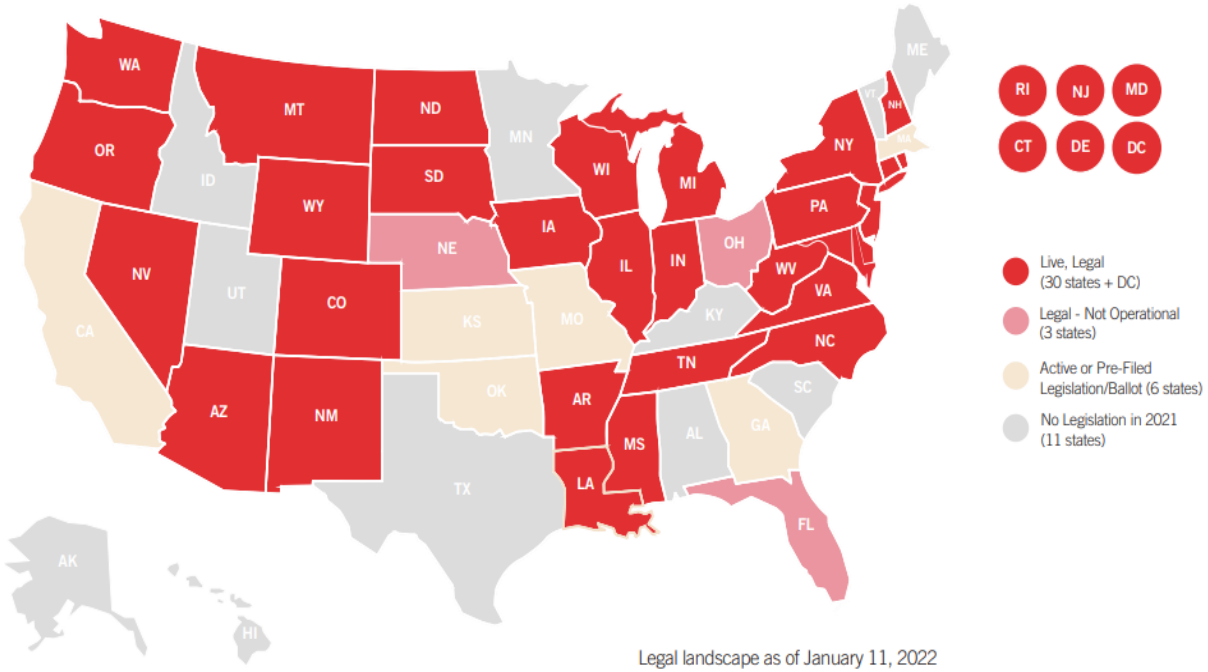
GIBSON DUNN

# Sports Betting and Online Gambling

# Sports Betting and Online Gambling
*Key Developments*

***Murphy v. National Collegiate Athletic Association* (2018)**, argued by Gibson Dunn at the Supreme Court, removed the prohibition on sports betting under federal law.

## Legal Sports Betting in the U.S.



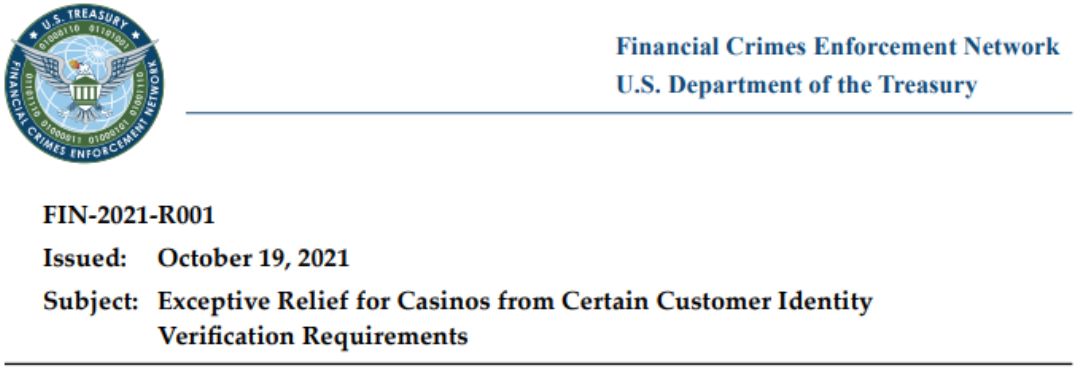

Legal landscape as of January 11, 2022

**Source: American Gaming Association**

- In the past 12 months, the number of states that have legalized sports betting has grown from **19 (plus DC) to 33.** Six additional states have active or pre-filed legislation for 2022 to legalize sports betting.
- Americans placed $42.19 billion in sports betting wagers from January to October 2021, double the wagers placed during that period in 2020.
- Sports betting conducted through casinos is subject to the BSA program, reporting, and recordkeeping requirements.

# Sports Betting and Online Gambling
## *FinCEN Exceptive Relief*

- In October 2021, FinCEN released guidance creating **exceptions to certain customer identification requirements in the context of online gaming**.
- Because casinos are not subject to Customer Identification Program ("CIP") regulations, they typically are not permitted to rely upon non-documentary verification of a customer's identity.
- FinCEN recognized that the onboarding procedures for online customers used by many brick and mortar casinos, which may include non-documentary identity verification, can provide more comprehensive verification of an online patron's identity than the procedures currently required under FinCEN rules.



Financial Crimes Enforcement Network
U.S. Department of the Treasury

FIN-2021-R001

Issued: October 19, 2021

Subject: Exceptive Relief for Casinos from Certain Customer Identity Verification Requirements

# Sports Betting and Online Gambling
## *FinCEN Exceptive Relief*

- In recognition of the fact that new types of gaming, such as online gambling and sports betting, involve remote interaction with customers, FinCEN granted certain limited exceptions to allow verification through non-documentary means, which could include:
  - Communications with the customer;
  - Verification through comparison of information from the customer with other information from public databases;
  - Reference checks with other financial institutions; and/or
  - Review of financial documents.
- FinCEN's exceptive relief does not modify state rules and states may impose more stringent verification requirements.
- A casino's BSA/AML program must describe when the casino will verify identity through documentary and/or non-documentary methods and address circumstances which non-documentary procedures may pose greater risks.

GIBSON DUNN

# U.S. Measures Involving China

# OFAC Guidance to Industry:
## *Xinjiang and Hong Kong Advisories*

- On July 13, the U.S. Departments of State, Treasury, Commerce, Homeland Security, and Labor issued an expanded advisory on the reputational, economic, and legal risks of engaging with parties implicated in rights abuses in, or linked to, China's **Xinjiang Uyghur Autonomous Region**.
  - Details practices by PRC authorities that the U.S. Government considers objectionable, including especially related to **forced labor** and **mass surveillance**.
  - Identifies "red flags" that individuals or entities linked to Xinjiang may be using forced labor, including dealing in certain types of goods (e.g., cotton, polysilicon) or operating facilities located within or near known internment camps or prisons.
  - Urges businesses and individuals to conduct enhanced **human rights due diligence** to identify potential supply chain links to entities operating in, or with ties to, Xinjiang.
  - Offers compendium of relevant U.S. legal authorities and recent actions targeting Xinjiang.
- On July 16, a similar group of U.S. Government agencies issued related guidance describing the risks that can arise from operating in **Hong Kong**, including arrest under the Hong Kong national security law, warrantless electronic surveillance, and restrictions on the flow of information.
  - Warns that businesses may suffer consequences for complying with U.S. sanctions measures under China's new counter-sanctions law.

*Photo source: Council on Foreign Relations cfr.org*

# U.S. Measures Against China
## *A Continued "Whole of Government" Approach*

***Congressional Action:***

- **Act Forbidding Entry of Goods into the U.S. Made with Forced Labor in the Xinjiang Uyghur Autonomous Region** (Pub. L. 117-78), signed December 23, creates a "rebuttable presumption" that all goods manufactured in Xinjiang are made with forced labor, unless the U.S. Customs and Border Protection certifies otherwise.
  - The Forced Labor Enforcement Task Force established under the USMCA Implementation Act is charged with drafting policies to implement the measures described.

***Presidential Action:***

- On June 3, President Biden signed **EO 14031** ("Addressing the Threat From Securities Investments That Finance Certain Companies of the People's Republic of China"), which expanded the potential application of the Non-SDN Chinese Military-Industrial Complex Companies List (the "NS-CMIC List") to China's defense and related materiel sector and surveillance technology sector, as well as companies owned or controlled by, directly or indirectly, a person who operates or has operated in such sectors.
- On June 9, 2021, President Biden signed **EO 14034** ("Protecting Americans' Sensitive Data From Foreign Adversaries") targeting foreign adversaries attempts to steal the personal data of U.S. citizens. The EO specifically names China as a national security threat and aligns with the ongoing emergency declared by then-President Trump in EO 13873 (May 2019).
- On December 6, President Biden announced a **diplomatic boycott** of the 2022 Winter Olympics in Beijing.

**U.S. Department of Justice (DOJ) China Initiative:**

- DOJ maintained an enforcement priority for cases arising out of China, including **prosecuting cases for trade secret theft, economic espionage, and facilitation of illegal exports** in 2021.

# U.S. Measures Against China
## *A Continued "Whole of Government" Approach*

***U.S. Customs and Border Protection (CBP):***

- On January 13, CBP issued a withhold release order (WRO), effectively **banning all cotton and tomato products** from the Xinjiang region from import into the United States.
- On June 23 CBP issued a WRO against Hoshine Silicon Industry Co. Ltd., a **solar panel material manufacturer based in the Xinjiang region**, over forced labor concerns.

***U.S. Federal Communications Commission (FCC):***

- On March 12, the FCC **prohibited the use of federal subsidies to purchase equipment or services from five Chinese telecom companies**, including Huawei, ZTE, Hytera, Hikvision, and Dahua.
- On March 17, the FCC initiated a proceeding to determine if **China Unicom Americas** business licenses should be revoked.
- On October 26, the FCC **revoked China Telecom America's services authority**, effectively banning the company from providing telecom services in the U.S.

***U.S. Department of Treasury:***

- On March 17, OFAC sanctioned 24 individuals, including the ranking Vice-Chairperson of the Standing Committee of the National People's Congress, under the **Hong Kong Autonomy Act** for materially contributing to China's failure to meet its obligations under the Sino – British Joint Declaration. Additional designations occurred on January 15 and July 16.
- On March 22, OFAC designated two current Chinese government officials in connection with serious human rights abuses against ethnic minorities in the Xinjiang region under the **Global Magnitsky Act.** Additional designations of two more government officials occurred on December 10.
- On June 3, in conjunction with the signing of EO 14031, OFAC added 58 new entities to the **NS-CMIC List**. Additional designations occurred on December 10 and December 16.



*Photo credit: Council on Foreign Relations cfr.org*

# U.S. Measures Against China
## *A Continued "Whole of Government" Approach*

***Securities and Exchange Commission ("SEC"):***

- On December 2, the SEC finalized rules to **ban companies from trading in the U.S. securities markets** if the Public Company Accounting Oversight Board ("PCAOB") is unable to inspect the audits of such companies for three consecutive years. This rule is largely seen as giving the SEC the power to delist Chinese firms who do not adequately disclose government ties.

***U.S. Department of Commerce:***

- On January 14, BIS added **China National Offshore Oil Corporation Ltd. to the Entity List** and Beijing Skyrizon Aviation Industry Investment Co., Ltd. to the Military End-User List.
- On January 15, BIS issued an **expanded military-intelligence end user rule (15 C.F.R. § 744.22)** prohibiting U.S. persons from supporting a "military-intelligence end use" or a "military-intelligence end user" in China, Iran, North Korea, Russia, Syria, or Venezuela without a license from BIS. Licenses are reviewed with a presumption of denial, and the rule came into effect on March 16.
- On April 8, BIS added **7 Chinese supercomputing companies to the Entity List** for supporting China's military actors and their modernization and their "destabilizing military modernization efforts."
- On June 24, 2021, BIS added 5 Chinese companies to the Entity List **for alleged violations of human rights and the use of forced labor** in the Xinjiang region.
- On July 12, BIS added 23 Chinese companies and entities – 14 over their role in **alleged human rights abuses in the Xinjiang region**, 5 for their **ties to China's military**, and another 4 **exporting items subject to the EAR without a license**.
- On November 26, BIS added **12 Chinese companies, including some quantum computing companies**, for their ties to China's military and military end-use activity.
- On December 17, BIS added an additional **34 more Chinese entities** to the Entity List for their **ties to China's military and military end-use activity.**

# U.S. Measures Against China
## *WeChat and TikTok Update*


- In November 2019, the Committee on Foreign Investment in the U.S. ("**CFIUS**") began reviewing the acquisition by ByteDance, TikTok's Chinese parent company, of Music.ly, TikTok's predecessor, to determine whether that transaction presented national security concerns.
- Before the CFIUS case concluded, then-President Trump intervened in early August 2020, announcing in two executive orders that the Commerce Department would impose restrictions not only on **TikTok**-related transactions but also on transactions involving **WeChat**—another Chinese-owned mobile app.
  - Before these restrictions could come into effect, federal judges in three cases blocked their implementation on the grounds that the President may have overstepped his IEEPA authorities or violated users' first amendment rights—suggesting a rare restriction on the President's expansive sanctions authority.
  - On June 9, 2021, President Biden revoked his predecessor's executive orders imposing restrictions on **TikTok** and **WeChat.**
  - The court cases challenging these executive orders were subsequently dismissed.
- The review of ByteDance's acquisition of Music.ly by **CFIUS remains ongoing**, and in the interim, the case challenging CFIUS's review remains in abeyance while the parties remain "**involved in ongoing negotiations.**"

# China's Latest Movements
## *Recent Responses to U.S. Actions*

- ***January 2021***
  - China issued **new blocking measures** in accordance with its **National Security Law** meant to counter the extraterritorial reach of foreign government sanctions and related foreign court rulings
  - China's **"Measures for the Security Review of Foreign Investment"** came into effect, which outline a legal framework for China's national security review of foreign investment similar to the U.S.'s CFIUS regime.
  - China's Ministry of Industry and Information Technology issued draft **"Regulations on Rare Earth Management"** that limit the export of rare earth elements and put these materials often used in technology devices including smartphones and batteries under the purview of China's Export Control Law
  - China issued **sanctions against 28 Trump administration officials**, including former Secretary of State Mike Pompeo, for undermining China's interests and disrupting China-U.S. relations
- ***June 2021***
  - China adopted an **Anti-Foreign Sanctions Law**, which centralizes China's existing authorities and formalizes the government's ability to sanction and countersanction individuals, entities, and governments, as well as impose countermeasures in response to other countries' sanctions.
  - China adopted a new **Data Security Law** aimed at managing and protecting data according to state interests and restricting the transfer or data outside of China's borders without government approval. This law entered into effect on September 1.

# China's Latest Movements
*Recent Responses to U.S. Actions*

- ***July 2021***
  - In July 2021, China's State Council issued new "**Regulations on the Security Protection of Critical Information Infrastructure**" to prioritize the protection of critical information infrastructure both in China and overseas. The regulations require network operations to report major incidents and intrusions and call for the joint military and civilian protection of critical information infrastructure.
  - On July 23, in response to the issuance of the U.S. government's "Hong Kong Business Advisory" and sanctioning of Chinese officials in July 2021, China **imposed sanctions on six U.S. citizens, including former Secretary of Commerce Wilbur Ross, and one U.S. entity, the Hong Kong Democratic Council.**

# Some Signs of Rapprochement
## *A Pivot in the Biden-Xi Relationship?*

- ***Bilateral Discussions***
  - In March, Secretary of State Antony Blinken and National Security Advisor Jake Sullivan met with senior Chinese foreign policy official Yang Jiechi and Foreign Minister Wang Yi in Anchorage, Alaska, for **bilateral talks.**
  - In April US Special Presidential Envoy for Climate John Kerry and China Special Envoy for Climate Change Xie Zhenhua met in China to discuss **joint climate change initiatives**.
  - In October, Jake Sullivan and Yang Jiechi re-engaged in **bilateral discussions** in Zurich.
  - In November, President Biden and President Xi participated in a **virtual summit** to discuss a wide array of topics, including Taiwan, trade, and human rights.
  - Throughout 2021, various high level officials including Secretary of the Treasury Janet Yellen, U.S. Trade Representative Katherine Tai, and US Secretary of Commerce Gina Raimondo engaged in **bilateral discussions** with their Chinese counterparts.

# Some Signs of Rapprochement
## *A Pivot in the Biden-Xi Relationship?*

- ***Some Easing Restrictions and Joint Action***
  - In March, the Office of the US Trade Representative **extended tariff exclusions** for some medical products from China needed to address the COVID-19 pandemic.
  - In August, the Commerce Department **allegedly approved licenses for Huawei to buy computer chips** for its auto component business.
  - In September, China **extended tariff exemptions on 81 products from the U.S.** and **Huawei CFO Meng Wanzhou is permitted to return** to China after almost 2 years of detention in Canada on U.S. fraud charges.
  - In November, the US and China announce a **joint declaration on action to address climate change.**

GIBSON DUNN

# Panelists

# F. Joseph Warin

1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306, USA
Tel: +1 202.887.3609
FWarin@gibsondunn.com

F. Joseph Warin is chair of the nearly 200-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. Mr. Warin'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.

Mr. Warin 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. *Who's Who Legal* named Mr. Warin a "Global Elite Thought Leader" in its 2020 and 2019 Investigations guides list for Business Crime Defense - Corporate and Investigations. In 2018, Mr. Warin 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 Mr. Warin 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 - 2020 for White Collar Criminal Defense. *U.S. Legal 500* has repeatedly named him as a "Leading Lawyer" for Corporate Investigations and White Collar Criminal Defense Litigation. He has been recognized by *Benchmark Litigation* as a U.S. White Collar Crime Litigator "Star" for ten consecutive years (2011-2020), and was named to *Securities Docket's* "Enforcement 40" for 2017.

Mr. Warin's group was recognized by *Global Investigations Review* in 2019 as the leading global investigations law firm in the world. This is the fourth time in five years to be so named. *Global Investigations Review* reported that Mr. Warin has now advised on more FCPA resolutions than any other lawyer since 2008. *Best Lawyers®* named Mr. Warin the Lawyer of the Year in 2020 and in 2016 for White Collar Criminal Defense in the District of Columbia, and he was named among the *Lawdragon* 500 Leading Lawyers in America in 2016.

Mr. Warin 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). He has been hired by audit committees or special committees of public companies to conduct investigations into allegations of wrongdoing in a wide variety of industries including energy, oil services, financial services, healthcare and telecommunications.

Mr. Warin's civil practice includes representation of clients in complex litigation in federal courts and international arbitrations. He has tried 10b-5 securities and RICO claim lawsuits, hostile takeovers and commercial disputes. He has handled more than 40 class action cases across the United States for investment banking firms, global corporations, Big 4 accounting firms, broker-dealers and hedge funds.

Early in his career, Mr. Warin served as Assistant United States Attorney in Washington, D.C. As a prosecutor, he tried more than 50 jury trials and was awarded a Special Achievement award by the Attorney General. Mr. Warin was awarded the Best FCPA Client Service Award by Main Justice in 2013 and he joined the publication's FCPA Masters list. He was named a Special Prosecutor by the District of Columbia Superior Court in 1988.

# Stephanie L. Brooker

1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306, USA
Tel: +1 202.887.3502
SBrooker@gibsondunn.com

Stephanie L. Brooker, former Director of the Enforcement Division at the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) and a former federal prosecutor, is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher. She is Co-Chair of the firm's White Collar Defense and Investigations, the Financial Institutions, and the Anti-Money Laundering Practice Groups. As a prosecutor, Ms. Brooker tried 32 criminal trials, investigated a broad range of white collar and other federal criminal matters, briefed and argued criminal appeals, and served as the Chief of the Asset Forfeiture and Money Laundering Section in the U.S. Attorney's Office for the District of Columbia. Ms. Brooker has been named a National Law Journal White Collar Trailblazer and a Global Investigations Review Top 100 Women in Investigations.

Ms. Brooker'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, multi-national companies, and individuals in connection with criminal, regulatory, and civil enforcement actions involving sanctions; anti-corruption; anti-money laundering (AML)/Bank Secrecy Act (BSA); securities, tax, and wire fraud, foreign influence; "me-too;" cryptocurrency; and other legal issues. She routinely handles complex cross-border investigations. Ms. Brooker's practice also includes BSA/AML and FCPA compliance counseling and deal due diligence and significant criminal and civil asset forfeiture matters.

Ms. Brooker'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.

Ms. Brooker served as an Assistant U.S. Attorney in the U.S. Attorney's Office for the District of Columbia, where she served for many years as a trial attorney in Federal and Superior Court. In the latter part of her tenure, she served as the first Chief of the new Asset Forfeiture and Money Laundering Section. This Section was responsible for all asset forfeiture and money laundering issues in Criminal Division cases and for litigation of civil forfeiture cases. In this role, she investigated and prosecuted complex civil and criminal forfeiture cases involving high-priority enforcement areas, such as national security, sanctions violations, and major financial fraud. She established the USAO's first DC Financial Crimes Task Force and supervised the investigation and prosecution of BSA and money laundering cases. During her tenure, she received the U.S. Attorney's Award for Creativity and Innovation in Management. She was also awarded three Special Achievement Awards for Superior Performance and the Office's Criminal Division Award.

Ms. Brooker also served as the first Director of FinCEN's Enforcement Division, which is the lead federal regulator with responsibility for enforcing the U.S. AML laws and regulations. In this role, she oversaw all of FinCEN's domestic and foreign enforcement and compliance under the BSA. She also oversaw rulemaking actions under Section 311 of the PATRIOT Act against foreign institutions and jurisdictions, Geographic Targeting Orders, and examination and enforcement actions against cryptocurrency companies following FinCEN's 2013 cryptocurrency guidance. Prior to serving as Enforcement Director, Ms. Brooker served as Chief of Staff and Senior Advisor to the Director of FinCEN.

# Adam M. Smith

1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306, USA
Tel: +1 202.887.3547
ASmith@gibsondunn.com

Adam M. Smith is a partner in the Washington, D.C., office of Gibson, Dunn & Crutcher. He is an experienced international lawyer with a focus on international trade compliance and white collar investigations, including with respect to federal and state economic sanctions enforcement, CFIUS, the Foreign Corrupt Practices Act, embargoes, and export controls. *In 2019 and 2020, Mr. Smith was ranked nationally by Chambers USA as a leading attorney in International Trade: Export Controls & Economic Sanctions. Mr. Smith was also identified by Global Investigations Review as one of the leading sanctions practitioners in Washington, DC.*

From 2010-2015 Mr. Smith served in the Obama Administration as the Senior Advisor to the Director of the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and as the Director for Multilateral Affairs on the National Security Council. At OFAC he played a primary role in all aspects of the agency's work, including briefing Congressional and private sector leadership on sanctions matters, shaping new Executive Orders, regulations, and policy guidance for both strengthening sanctions (Russia and Syria) and easing measures (Burma and Cuba), and advising on enforcement actions following sanctions violations.

Mr. Smith travelled extensively in Europe, the Middle East, Asia, Africa, and the Americas conducting outreach with governments and private sector actors on sanctions, risk, and compliance. This outreach included meetings with senior leadership in several sectors including finance, logistics, insurance and reinsurance, energy, mining, technology, and private equity.

Mr. Smith frequently chaired the Treasury delegation to EU/G7 consultations regarding Russia sanctions and negotiated with EU institutions and member states to implement coordinated measures. Additionally, Mr. Smith managed the development and implementation of the U.S. government's international outreach program on Congressionally mandated Iran sanctions and helped develop proposed sanctions relief strategies as a part of the Iranian nuclear negotiations.

During Mr. Smith's tenure on the White House's National Security Council, he advised the President on his multilateral agenda including with respect to international sanctions, coordinated inter-agency efforts to relieve U.S. economic restrictions on Burma, and developed strategies to counter corruption and illicit flows and to promote stolen asset recovery.

# M. Kendall Day

1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306, USA
Tel: +1 202.955.8220
KDay@gibsondunn.com

M. Kendall Day is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher. He is a member of the White Collar Defense and Investigations and the Financial Institutions Practice Groups. Mr. Day's practice focuses on internal investigations, regulatory enforcement defense, white-collar criminal defense, and compliance counseling. He represents multi-national companies, financial institutions, 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, and sensitive employee matters. Mr. Day's practice also includes AML/BSA compliance counseling and due diligence, and the defense of forfeiture matters.

Prior to joining Gibson Dunn, Mr. Day spent 15 years 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, Mr. Day had responsibility for approximately 200 prosecutors and other professionals. Mr. Day 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, Mr. Day 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, Mr. Day served as a deputy chief and trial attorney in the Public Integrity Section of the DOJ. During his tenure at the Public Integrity Section, Mr. Day 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. From 2003 to 2005, he served as an Honors Program Trial Attorney in the DOJ's Tax Division. Mr. Day also served overseas as the Justice Department's Anti-Corruption Resident Legal Advisor in Serbia.

Mr. Day received a number of awards while at the DOJ, including the Attorney General's Award for Distinguished Service, the second highest award for employee performance; the Assistant Attorney General's Award for Exceptional Service; and the Assistant Attorney General's Award for Ensuring the Integrity of Government.

Mr. Day clerked for Chief United States District Court Judge Benson E. Legg of the District of Maryland. He earned his J.D. from the University of Virginia School of Law, where he graduated in 2002 after winning first place in the Lile Moot Court Competition and being selected to receive the Margaret G. Hyde Graduation Award. He graduated with honors and highest distinction from the University of Kansas in 1999 with a B.A. in Italian Literature and Humanities.

# Ella Alves Capone

1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306, USA
Tel: +1 202.887.3511
ECapone@gibsondunn.com

Ella Alves Capone is a senior associate in the Washington, D.C. office of Gibson, Dunn & Crutcher. She is a member of the White Collar Defense and Investigations and Anti-Money Laundering practice groups. Her practice focuses primarily in the areas of white collar criminal defense and corporate compliance.

Ms. Capone regularly conducts internal investigations and advises multinational corporations and financial institutions, including major banks and casinos, on compliance with anti-corruption and anti-money laundering laws and regulations. She has significant experience representing clients in white collar and securities matters involving the U.S. Department of Justice (DOJ), U.S. Securities and Exchange Commission (SEC), Financial Crimes Enforcement Network (FinCEN), Office of the Comptroller of the Currency (OCC), Office of Foreign Assets Control (OFAC), and the Federal Reserve Board. Additionally, Ms. Capone has experience representing individuals and financial institutions in a variety of criminal and civil litigation, particularly including alleged securities fraud.

Ms. Capone's practice additionally includes advising clients on the effectiveness of their internal controls and compliance programs, as well as conducting and advising on compliance due diligence for corporate deals.

Ms. Capone regularly works on international matters, with particular expertise in Latin America. Her representative matters include several anti-corruption and corporate compliance matters in Brazil. She is proficient in Portuguese and regularly uses Portuguese in professional contexts.

Ms. Capone frequently writes and presents on anti-corruption and compliance issues. Her recent written work includes the 2018 edition of Bloomberg BNA's Securities Practice Series Portfolio No. 285, The U.S. Foreign Corrupt Practices Act: Enforcement and Compliance; the 2017, 2018, 2019, and 2020 ABA Treatise, Practice Under the Federal Sentencing Guidelines; and ICLG To: Anti-Money Laundering 2018, USA.

Ms. Capone graduated from New York University School of Law in 2011, where she was a member of the Honorary Moot Court Board. She graduated summa cum laude and with departmental honors for all years from Fordham University, where she earned a dual degree in Psychology and Sociology and was inducted into Phi Beta Kappa. Prior to joining Gibson Dunn, she practiced at a major international law firm in Washington, D.C. and New York, where she specialized in white collar criminal defense, securities litigation, and internal investigations.

Ms. Capone is admitted to practice law in the District of Columbia and New York, as well as before the United States District Courts for the Eastern and Southern Districts of New York.

# Acknowledgements

The panelists would like to extend our thanks to our excellent colleagues who contributed to this webcast.

Douglas Colby is a litigation associate in the Washington, D.C. office. Prior to joining Gibson Dunn, Mr. Colby clerked for the Honorable Jerry E. Smith of the U.S. Court of Appeals for the Fifth Circuit. Mr. Colby received his law degree *cum laude* from Harvard Law School.

Melissa L. Farrar is a senior associate with experience representing and advising multinational corporations in internal and government investigations on a wide range of topics, including compliance with the U.S. Foreign Corrupt Practices Act and other anti-corruption laws, anti-money laundering, and tax.

Chris R. Mullen is an associate with experience advising clients on international trade matters related to corporate mergers and acquisitions, as well as compliance with anti-money laundering obligations at the state and federal levels.

Monica M. Murphy is an associate in the Washington, D.C. office. Her practice focuses on labor and employment, class action litigation, and white collar investigations. Ms. Murphy graduated from the University of Pennsylvania Carey Law School, where she served as the Managing Editor of the *University of Pennsylvania Law Review*.

Madelyn Mae La France is an associate in the firm's Litigation Department with experience conducting internal investigations involving alleged securities and accounting fraud, violations of the Foreign Corrupt Practices Act, and violations of anti-money laundering laws.

Tory Roberts is an associate in the Washington, D.C. office. Ms. Roberts received her Juris Doctor from Columbia Law School, where she received the Hamilton Fellowship, a merit-based full tuition scholarship. During law school, Ms. Roberts served as an Articles Editor for the *Columbia Law Review*.

Susanna G. Schuemann is an associate in the San Francisco office with experience advising multinational companies across a variety of industries with internal investigations, regulatory inquiries, and complex commercial litigation matters.

Audi K. Syarief is an associate with extensive experience in assessing enforcement and designation risk, conducting internal investigations, strengthening trade compliance programs, and securing licenses and other authorizations from OFAC.

Scott R. Toussaint is an associate with experience advising clients on matters before the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), the Committee on Foreign Investment in the United States (CFIUS), and other regulatory and enforcement agencies.

# Programs and Resources

- REGISTER: FCPA 2021 Year-End Update, Feb. 1st
- Webcast: Managing Internal Audit and Investigations
- Gibson Dunn Anti-Money Laundering Practice
- Subscribe to Gibson Dunn Alerts

# Our Offices

**Beijing**
Unit 1301, Tower 1
China Central Place
No. 81 Jianguo Road
Chaoyang District
Beijing 100025, P.R.C.
+86 10 6502 8500

**Brussels**
Avenue Louise 480
1050 Brussels
Belgium
+32 (0)2 554 70 00

**Century City**
2029 Century Park East
Los Angeles, CA 90067-3026
+1 310.552.8500

**Dallas**
2001 Ross Avenue, Suite 2100
Dallas, TX 75201-2923
+1 214.698.3100

**Denver**
1801 California Street
Denver, CO 80202-2642
+1 303.298.5700

**Dubai**
Building 5, Level 4
Dubai International Finance Centre
P.O. Box 506654
Dubai, United Arab Emirates
+971 (0)4 370 0311

**Frankfurt**
TaunusTurm
Taunustor 1
60310 Frankfurt
Germany
+49 69 247 411 500

**Hong Kong**
32/F Gloucester Tower, The Landmark
15 Queen's Road Central
Hong Kong
+852 2214 3700

**Houston**
811 Main Street, Suite 3000
Houston, TX 77002
+1 346.718.6600

**London**
Telephone House
2-4 Temple Avenue
London EC4Y 0HB
England
+44 (0) 20 7071 4000

**Los Angeles**
333 South Grand Avenue
Los Angeles, CA 90071-3197
+1 213.229.7000

**Munich**
Hofgarten Palais
Marstallstrasse 11
80539 Munich
Germany
+49 89 189 33-0

**New York**
200 Park Avenue
New York, NY 10166-0193
+1 212.351.4000

**Orange County**
3161 Michelson Drive
Irvine, CA 92612-4412
+1 949.451.3800

**Palo Alto**
1881 Page Mill Road
Palo Alto, CA 94304-1125
+1 650.849.5300

**Paris**
166, rue du faubourg Saint Honoré
75008 Paris
France
+33 (0)1 56 43 13 00

**San Francisco**
555 Mission Street
San Francisco, CA 94105-0921
+1 415.393.8200

**São Paulo**
Rua Funchal, 418, 35°andar
Sao Paulo 04551-060
Brazil
+55 (11)3521.7160

**Singapore**
One Raffles Quay
Level #37-01, North Tower
Singapore 048583
+65.6507.3600

**Washington, D.C.**
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306
+1 202.955.8500