February 7, 2024

BSA/AML AND INTERNATIONAL TRADE ENFORCEMENT AND COMPLIANCE ANNUAL UPDATE

GIBSON DUNN

MCLE Credit

- Approved for 2.0 hours General PP credit in NY, CA, and CT.
- Approved for 2.0 CPD Credit by Solicitors Regulation Authority.
- Approval pending for 2.0 hours General PP Credit in CO, IL, TX, VA, and WA.
- CLE credit form must be submitted using the below link by **Wednesday, February 14th.** The announced CLE Code will need to be entered in the form.
  - Form Link: https://gibsondunn.qualtrics.com/jfe/form/SV_bKloCERqJj1WUCy
- Most participants should anticipate receiving their certificate of attendance in four to eight weeks following the webcast.
- **Please direct all questions regarding MCLE to CLE@gibsondunn.com.**

Agenda

01	Overview of Current AML and International Trade Landscape and Risks of Focus
02	Rulemaking and Legislative Developments
03	BSA/AML and International Trade Enforcement Actions
04	Compliance Best Practices and Regulatory Expectations
05	Expectations for 2024 and Beyond

OVERVIEW OF CURRENT LANDSCAPE AND RISK AREAS OF FOCUS

01

U.S. AML and Sanctions Regulators and Enforcers

Primary AML and Sanctions Regulators

FinCEN

OFAC

State Regulators

Secondary AML and Sanctions Regulators

Banking Regulators (OCC, Fed, FDIC, NCUA)

CFTC

SEC

FINRA

Enforcers

DOJ Criminal Division MLARS

National Security Division CES

U.S. Attorney's Offices

DOJ Civil Division CPB

Treasury and DOJ Key Personnel

Secretary
Janet Yellen
(Senate Confirmed)

Deputy Secretary
Wally Adeyemo
(Senate Confirmed)

Under Secretary for Terrorism and Financial Intelligence
Brian Nelson
(Senate Confirmed)

FinCEN Director
Andrea Gacki

OFAC Director
Bradley Smith

Attorney General
Merrick B. Garland
(Senate Confirmed)

Deputy Attorney General
Lisa Monaco
(Senate Confirmed)

National Security Division Assistant Attorney General
Matthew Olsen
(Senate Confirmed)

Criminal Division Assistant Attorney General
Nicole M. Argentieri
(Acting)

Chief, Counterintelligence and Export Control Section
Jennifer Gellie
(Acting)

Chief, Money Laundering and Asset Recovery Section
Molly Moeser
(Acting)

RISK AREAS OF FOCUS: DIGITAL ASSETS

Focus on Digital Assets

- In March 2022, President Biden issued an **Executive Order on Ensuring Responsible Development of Digital Assets** that outlined a government approach to addressing the risks associated with virtual currencies and their underlying technologies.
- In September 2022, the **White House issued a Comprehensive Framework for the Responsible Development of Digital Assets** that highlighted how "digital assets…have been exploited by bad actors to launder illicit proceeds, to finance terrorism and the proliferation of weapons of mass destruction and to conduct a wide array of other crimes" and called for expanded regulation of the industry and increased enforcement and penalties for regulatory violations by those within the industry.

"Fostering responsible innovation in the cryptocurrency industry has long been a top priority of ours. Responsible innovation, to us, means innovation that has compliance embedded in its DNA. Innovation that is executed in a way that is mindful of and helps to protect our national security interests and to protect people from harm."

Himamauli Das
FinCEN Acting Director
April 27, 2023

Focus on Digital Assets

Decentralized Finance

In April 2023, Treasury published its "2023 DeFi Illicit Finance Risk Assessment" in response to the mandate from the September 2022 White House Report. The Risk Assessment noted significant risks in decentralized finance, with a particular focus on:

- AML regulatory gaps for decentralized finance businesses.
- Lack of AML regulatory compliance by covered decentralized finance businesses.
- Increasing use of decentralized finance solutions by bad actors to move illicit funds anonymously.

Accordingly, Treasury recommended:

- Strengthening U.S. AML regulatory supervision.
- Considering additional guidance for the private sector on decentralized finance AML obligations.
- Enhancements to address AML regulatory gaps related to decentralized finance solutions.

RISK AREAS OF FOCUS: FINTECHS AND PAYMENTS

Focus on Fintech Relationships

Regulators have continued to take an increased focus on relationships between fintechs and depository institutions, emphasizing the need for depository institutions to take risk-based approaches to the relationships and measures to ensure the institution's BSA/AML compliance is not compromised by the relationship, including, but not limited to:

- Due diligence of the fintech prior to entering into a relationship;
- Adequate contract terms with the fintech that identify each parties obligations, provide the depository institution with monitoring, auditing, and termination rights as needed for compliance;
- BSA/AML training, particularly if the fintech assists with any part of the institution's BSA/AML compliance program; and
- Monitoring and oversight of the fintech's activities throughout the relationship.

Several guidance documents on these third-party relationships have been published by the OCC, Federal Reserve, and FDIC over the past two years, with the most recent on June 5, 2023, and there have been several enforcement actions over the past year related to banks' relationships with fintechs.

In April 2023, OCC established its Office of Financial Technology, which seeks "to ensure the agency's leadership and agility in providing high-quality supervision of bank-fintech partnerships…[and] enhances the agency's knowledge and expertise of financial technology platforms and applications in support of the OCC's mission."

RISK AREAS OF FOCUS:
SANCTIONS AND TRADE CONTROLS EVASION

Treasury's Stance on Sanctions Issues

Throughout 2023, the Biden Administration leveraged its sanctions toolbox to put economic pressure on countries including Russia and Iran in order to further its foreign policy and national security goals.

"No one should doubt the resolve of the United States and our partners when weighing the real risks associated with support for Russian evasion. We expect financial institutions will undertake every effort to ensure that they are not witting or unwitting facilitators of circumvention and evasion. And we will not hesitate to . . . take decisive, and surgical, action against financial institutions that facilitate the supply of Russia's war machine."

Janet L. Yellen
Secretary of the Treasury
December 22, 2023

"Iran's continued, deliberate proliferation of its UAVs enables Russia, its proxies in the Middle East, and other destabilizing actors to undermine global stability. The United States will continue to take action against Iran's UAV procurement networks, and encourages jurisdictions to exercise the due diligence necessary to prevent the export of these components to Iran."

Brian E. Nelson
Under Secretary of the Treasury for Terrorism & Financial Intelligence
September 19, 2023

OFAC

Treasury's Sanctions Policy Review

In October 2021, the Treasury Department issued a comprehensive Sanctions Review, outlining several principles to guide U.S. sanctions policy. These principles are evident in the Biden Administration's sanctions approach to date.

- **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.

Focus on Sanctions and Trade Controls Evasion Involving Russia

Since March 2022, FinCEN has regularly issued alerts, advisories, and bulletins relating to Russia:

- November 2023: FinCEN, OFAC, and BIS co-hosted a FinCEN Exchange to discuss attempts by Russia to evade export controls.
- September 2023: A Financial Trend Analysis from FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security (BIS) on patterns and trends contained in Bank Secrecy Act (BSA) reporting on suspected evasion of Russia-related export controls.
- May 2023: Alert urging continued vigilance on the part of U.S. financial institutions for potential attempts by Russia to evade U.S. export controls.
- January 2023: Alert regarding potential U.S. Commercial real estate investments by sanctioned Russian elites, oligarchs, and family.
- December 2022: Financial Trend Analysis showing Russia-related transactions reported in BSA filings indicative of corruption and sanctions evasion and involving shell companies, real estate, and high-valued goods.
- November 2022: Financial Trend Analysis showing ransomware-related incidents reported in BSA filings more than doubled between 2020 and 2021, with 75% and the top five highest grossing incidents involving Russia-related ransomware variants.
- June 2022: Alert advising increased vigilance for Russian and Belarusian export control evasion attempts.
- April 2022: Advisory regarding corruption and kleptocracy with focus on Russian actors and noting use of real estate, luxury goods, and shell companies to launder funds.
- March 2022: Alert regarding sanctions evasion activity involving Russia and associated red flags.

FinCEN Broadens Focus to Advanced and Critical Technologies Evasion

November 6, 2023 Joint Alert

"The purposeful evasion of U.S. export controls, regardless of where it occurs or the adversary it supports, is a serious national security issue."

FinCEN Director Andrea Gacki

FIN-2023-NTC2 November 6, 2023

Joint Notice **expands** on the red flags mentioned in previous notices that suggest sanctions evasion, with a particular focus on **global export control diversion** of **advanced and critical technologies** "that can be used in new or novel ways to enhance adversaries' military capabilities or support mass surveillance programs that enable human rights abuses."

Financial institutions are requested to use the following code to identify global evasion SARs: "FIN-2023-GLOBALEXPORT"	
Entities with no web presence or whose phone number area codes do not match destination country	Customer listed as consignee appears to be mail centers, trading companies, or logistics companies
Supporting documents do not list the end-user	Item does not fit the purchaser's line of business
Customer lacks or refuses to provide details to banks, shippers, or third parties	Customer significantly overpaying for item based on known market price

FinCEN Broadens Focus to Advanced and Critical Technologies Evasion

November 6, 2023 Joint Alert

FIN-2023-NTC2

November 6, 2023

*"The purposeful evasion of U.S. export controls, regardless of **where it occurs or the adversary it supports**, is a serious national security issue."*

FinCEN Director Andrea Gacki

Joint Notice **expands** on the red flags mentioned in previous notices that suggest sanctions evasion, with a particular focus on **global export control diversion** of **advanced and critical technologies** "that can be used in new or novel ways to enhance adversaries' military capabilities or support mass surveillance programs that enable human rights abuses."

Financial institutions are requested to use the following code to identify global evasion SARs: "FIN-2023-GLOBALEXPORT"

- Entities with no web presence or whose phone number area codes do not match destination country
- Customer listed as consignee appears to be mail centers, trading companies, or logistics companies
- Supporting documents do not list the end-user
- Item does not fit the purchaser's line of business
- Customer lacks or refuses to provide details to banks, shippers, or third parties
- Customer significantly overpaying for item based on known market price

Focus on Terrorist Financing Relating to Hamas

More recently, FinCEN has issued alerts and held roundtables regarding terrorist financing trends relating to Hamas:

- October 18, 2023: FinCEN announced a meeting with Israel's FIU regarding cooperation efforts and stated "FinCEN is redoubling its efforts to combat the financing of terrorism alongside IMPA and other strategic FIU partners during this critical time."
- October 20, 2023: FinCEN issued an alert advising financial institutions to be alert to red flags for Hamas-related financing.
- November 6, 2023: FinCEN held a public-private discussion on cyber-related terrorism financing that focused on Hamas-related financing attempts and strongly encouraged financial institutions to engage in 314(b) voluntary information sharing to better detect this type of activity.
- November 27, 2023: FinCEN publicly announced a task force created immediately after the October 7, 2023 attacks in Israel consisting of FIUs from 13 countries - Australia, Canada, Estonia, France, Germany, Israel, Liechtenstein, Luxembourg, the Netherlands, New Zealand, Switzerland, the United Kingdom, and the United States – "aim[ed] to strengthen efforts to disrupt international financial flows to Hamas and other terrorist organizations." The taskforce members committed to:
  - Enhance financial intelligence on terrorist-financing related matters and associated financial flows and economic activities;
  - Expedite and increase sharing of financial intelligence in terrorist financing-related matters and associated financial flows and economic activities;
  - Discuss FIU best practices, lessons learned, and opportunities for additional actions and partnerships to combat and disrupt terrorist financing activities; and
  - Strengthen and facilitate working relationships between FIUs and competent public authorities and the private sector addressing this threat.

RISK AREAS OF FOCUS: FENTANYL TRAFFICKING

Focus on Fentanyl Trafficking

In 2023, FinCEN engaged in multiple meetings with financial institutions and foreign counterparts to identify and combat illicit finance trends associated with fentanyl trafficking.

"FinCEN [] plays an important role in the whole-of-government effort to combat the trafficking of fentanyl and fentanyl precursor chemicals....We know that to tackle a problem like this, financial institutions and law enforcement agencies need to work together – the each have a critical role to play – and FinCEN has a role to play in building the bridges for these two groups to collaborate."

Andrea Gacki
FinCEN Director
October 2023

RISK AREAS OF FOCUS: CYBER CRIMES AND FRAUD

Regulator Focus on Cybercrimes and Fraud

DOJ, FinCEN, and other federal and state regulators have been focused on the adequacy of organizations' cybersecurity programs.

- Increased enforcement related to cybersecurity weaknesses.
- Increased state and federal regulations regarding cyber- and information security programs.

Regulators have also been increasingly focused on consumer protection efforts and consumer financial fraud that financial institutions should be alert to. Notable fraud trends in 2023 include:

- Check frauds
- "Pigbutchering" / Romance Scams
- Microtransaction fraud using online platforms
- Business Email Compromise
- Social Engineering on Social Media
- Online Marketplace frauds
- Identity fraud
- Ransomware and other extortion schemes, particularly involving cryptocurrencies
- Investment schemes

RULEMAKING AND LEGISLATIVE DEVELOPMENTS

02

RULEMAKING AND LEGISLATIVE DEVELOPMENTS: AML ACT OF 2020 IMPLEMENTATION

CTA Beneficial Ownership Reporting Final Rule

- **On September 29, 2022, FinCEN issued a final rule creating new beneficial ownership information reporting requirements for domestic and foreign companies, per the Corporate Transparency Act ("CTA") enacted in January 2021.**
  - Exempts public companies, SEC-registered issuers, MSBs registered with FinCEN, broker-dealers, and certain tax-exempt entities, among others.
- Requires reporting of identifying information to FinCEN regarding "beneficial owners" (defined as those who exercise substantial control over, or own and control at least 25% of the company) or "company applicants" (meaning those directly involved in or primarily responsible for the filing that creates the company).
  - Reporting Requirements: legal names, principal place of business, jurisdiction of formation, domestic or foreign tax identification numbers, BO dates of birth, BO addresses, and image of BO passport or other form of personal identification.
- Initial reports for all covered companies created prior to January 1, 2024 must be submitted by January 1, 2025, and covered companies must promptly update or correct outdated or inaccurate information.
  - November 29, 2023 Final Rule: Extending time for companies created after January 1, 2024 and before January 1, 2025 to file their reports from 30 days to 90 days. Companies created after January 1, 2025 will have 30 days to file.
- Willful violations of these reporting requirements can be subject to civil and criminal penalties, and liability can be attached to direct or indirect violations and for acts or omissions.

CTA Information Access and Safeguards Final Rule

- **On December 22, 2023, FinCEN issued its final rule governing the circumstances under which beneficial ownership information may be disclosed to various types of government authorities and financial institutions and required confidentiality measures.** This came almost exactly a year after its NPRM that was met with strong resistance by the banking community.
- Authorized Recipients:
  - **Financial Institutions can receive BOI to facilitate compliance with customer due diligence requirements under applicable law, if it has the company's consent. The Final Rule expanding "customer due diligence requirements under applicable law" to include "any legal requirement or prohibition designed to counter money laundering or the financing of terrorism, or to safeguard the national security of the United States, to comply with which it is reasonably necessary for a financial institution to obtain or verify beneficial ownership information of a legal entity customer." This may include any AML/CFT and sanctions compliance purposes, provided it is reasonably necessary to obtain or verify the BOI to satisfy those requirements. General business or commercial use of BOI is expressly prohibited.**
  - Federal agencies can receive BOI in furtherance of national security, intelligence, or criminal or civil law enforcement activity, and state, local, and tribal authorities can receive BOI if they have a court order authorizing them to seek the information in a criminal or civil investigation.
  - Federal functional regulators can receive BOI when acting in a supervisory capacity assessing financial institutions for compliance with CDD requirements, but they can only receive BOI the supervised financial institution received.
  - Foreign enforcement or government authorities can receive BOI if through an intermediary Federal agency, for law enforcement or national security purposes, and pursuant to a treaty or convention.
  - Treasury personnel have broad access to BOI data.

CTA Information Access and Safeguards Final Rule (Cont'd)

- **Phased Approach to BOI access**
  - Pilot program in 2024 for a handful of key Federal agencies
  - Treasury offices and certain Federal agencies engaged in law enforcement and national security activities that already have Memoranda of Understanding (MOUs) for access to BSA information
  - Additional Federal agencies engaged in law enforcement, national security, and intelligence activities, as well as to State, local, and Tribal law enforcement partners
  - Intermediary Federal agencies in connection with foreign government requests
  - Lastly, financial institutions and their supervisors
- **Type of Access**
  - Federal and state law enforcement and Treasury personnel: Direct access to BO system with unfettered query capabilities and immediate access to results
  - Foreign Recipients: No direct access; only through intermediary federal agencies.
  - Financial institutions and their regulators: Direct access to BO system, but in a more limited fashion than what U.S. federal and state law enforcement will have.
- **Required Safeguards**
  - "Financial institutions that obtain BOI from FinCEN must develop and implement administrative, technical, and physical safeguards reasonably designed to protect the information. Financial institutions will be able to satisfy this requirement by applying to BOI the same security and information handling procedures they use to protect customers' nonpublic personal information in compliance with section 501 of the Gramm-Leach-Bliley Act and its implementing regulations. For each BOI request that it makes, a financial institution will have to certify that the request satisfies applicable criteria. Certain geographic restrictions will also apply."

FinCEN AML/CFT Enforcement Priorities and Risk-Based AML Programs

On June 30, 2021, FinCEN published its first set of its AML/CFT enforcement priorities, which must be updated at least every four years:

- 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; and
- Proliferation financing.

As required by the AML Act, FinCEN will be publishing a NPRM (currently scheduled for March 2024) for new rules regarding how financial institutions must integrate these priorities into their AML programs.

- Per the Unified Regulatory Agenda, the NPRM will also include a **new risk assessment requirement.**
- This will be a measure "on which a financial institution is **supervised and examined**."
- Some regulators have indicated an expectation that institutions are already considering these priorities for their AML programs.

FinCEN ANPRM

No-Action Letter Process

On June 3, 2022, FinCEN issued an Advance Notice of Proposed Rulemaking (ANPRM) to solicit public comment on the implementation of a no-action letter process at FinCEN.

- Arises out of the AML Act of 2020.

Recognizes the plethora of parallel and overlapping authorities and seeks to supplement existing forms of regulatory guidance and relief.

AML Whistleblower Program

On December 23, 2022, the Anti-Money Laundering Whistleblower Improvement Act was enacted expanding the AML whistleblower program.

- Expanded to persons who report violations of U.S. sanctions laws and regulations;
- Guarantees that whistleblowers will be paid at least 10% of the value of fines collected as a result of the information they provide; and
- Creates a $300 million fund to pay whistleblower awards from fines collected by DOJ and Treasury.
- This has already reportedly resulted in a significant increase in AML-related whistleblower reports.
- Rulemaking in connection with this program is on the Unified Regulatory Agenda for 2024.

RULEMAKING AND LEGISLATIVE DEVELOPMENTS: EXPANSION OF BSA COVERAGE

Real Estate
NPRM

- **NPRMs for both residential and commercial real estate are expected this year and will seemingly impose transaction recordkeeping and reporting requirements on covered parties.**
  - Residential NPRM: Currently scheduled for February 2024
  - Commercial NPRM: Currently scheduled for September 2024

"For too long, the U.S. real estate market has been susceptible to manipulation and use as a haven for the laundered proceeds of illicit activity, including corruption. Our real estate market is a relatively stable store of value, and it can be opaque, and there are gaps in industry regulation. Increasing transparency in the real estate sector will assist with curbing the ability of corrupt officials and criminals to launder the proceeds of their illicit activity or ill-gotten gains as well as strengthen U.S. national security and help protect the integrity of the U.S. financial system. For that reason, Treasury is committed to developing a solution to increase the transparency in the domestic real estate market.…We are currently developing a Notice of Proposed Rulemaking [for the real estate industry]…"

Andrea Gacki
FinCEN Director
October 3, 2023

Investment Advisor NPRM

FinCEN is expected to issue a NPRM this year that will cover "certain" investment advisors and will seemingly include the full suite of AML program and SAR reporting requirements. The NPRM is currently scheduled in the unified regulatory agenda for February 2024.

This is part of a broader initiative to extend BSA coverage to gatekeepers and to combat corruption.

> **"Treasury will re-examine…minimum standards for anti-money laundering programs and suspicious activity reporting requirements for certain investment advisors. Certain types of investment professions and entities do not have comprehensive anti-money laundering obligations. This may allow corrupt actors to invest their ill-gotten gains in the U.S. financial system through hedge funds, trusts, private equity funds, and other advisory services or vehicles offered by investment advisers that focus on high-value customers. The lack of regulatory oversight of these industries means that, as the Treasury stated in its 2015 NPRM, 'it [is] possible for money launderers to evade scrutiny more effectively by operating through investment advisers rather than through broker-dealers or banks directly. In addition to re-examining the 2015 NPRM, the Treasury will further consider whether to cover private placement funds, including investments offered by hedge funds and private equity firms."**
>
> U.S. Strategy on Combatting Corruption, December 2021

Letter to Congress for Expanded Authorities to Combat Illicit Activity Involving Digital Assets

On November 28, 2023, Treasury sent Congress a letter describing increases in terrorist financing activity involving digital assets and requesting several types of expanded authorities in order to combat illicit use of digital assets.

- New secondary sanctions tool that would allow prohibitions on opening accounts for foreign cryptocurrency exchanges and financial service providers that facilitate payments to terrorist groups, akin to current Section 311 correspondent banking and payable through account special measures.
- Create a category under the BSA's "financial institution" definition for digital asset businesses, including but not limited to cryptocurrency exchanges, Virtual Asset Service Providers, virtual asset wallet providers, certain blockchain validator nodes, and decentralized finance services, and subject them to BSA requirements like other financial institutions.
- Create an explicit IEEPA authority to designate blockchain nodes, networks, or other elements of cryptocurrency transactions, rather than requiring that they be a designated person's property or interest in property.
- Explicitly provide for OFAC extraterritorial jurisdiction to assert authority over all transactions in stablecoin pegged to USD.
- Clarify that IEEPA jurisdiction extends to entities abroad with U.S. touchpoints.
- Clarify that BSA jurisdiction extends to entities abroad with U.S. touchpoints, but with option for substituted compliance for FATF-compliant jurisdictions.

RULEMAKING AND LEGISLATIVE DEVELOPMENTS: PRIMARY MONEY LAUNDERING CONCERNS

CVC Mixing NPRM

October 19, 2023, FinCEN published a NPRM pursuant to Section 311 that identifies international CVC Mixing as a class of transactions of primary money laundering concern and imposing special measures on financial institutions to implement certain recordkeeping and reporting requirements for transactions involving CVC Mixing.

"Today's action underscores Treasury's commitment to combatting the exploitation of Convertible Virtual Currency mixing by a broad range of illicit actors, including state-affiliated cyber actors, cyber criminals, and terrorist groups…More broadly, the Treasury Department is aggressively combatting illicit use of all aspects of the CVC ecosystem by terrorist groups, including Hamas and Palestinian Islamic Jihad."

FinCEN Bitzlato Order

Cryptocurrency

On January 18, 2023, FinCEN identified virtual currency exchange Bitzlato Limited (Bitzlato) as a "primary money laundering concern" in connection with Russian illicit finance.

- First time FinCEN used its authority under Section 9714(a) of the Combating Russian Money Laundering Act, which authorizes FinCEN to "prohibit, or impose conditions upon, certain transmittals of funds (to be defined by the Secretary) by any domestic financial institution or domestic financial agency, if such transmittal of funds involves any such institution, class of transaction, or type of account."

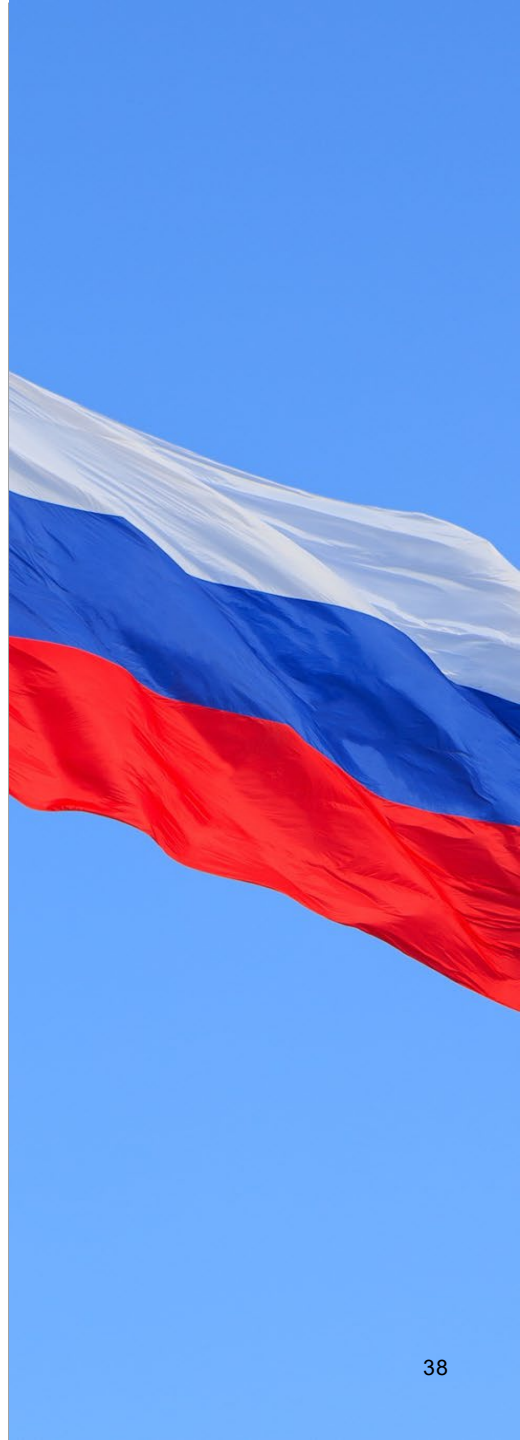
- The Bitzlato Order prevents, effective February 1, 2023, financial institutions from "engaging in a transmittal of funds from or to Bitzlato, or from or to any account or CVC address administered by or on behalf of Bitzlato."
- Bitzlato FAQs state that each covered financial institution should "exercise reasonable due diligence to prevent it (or its subsidiaries) from engaging in transmittals of funds involving Bitzlato."

RULEMAKING AND LEGISLATIVE DEVELOPMENTS: SANCTIONS

Russia

Since February 2022, the U.S. government has implemented an unprecedented range of sanctions and export controls targeting Russia's defense and military-industrial complex in response to that country's unprovoked attack on Ukraine.

- OFAC added **hundreds of Russian entities to the SDN List**, targeting entire sectors such as the financial sector (sanctioning banks representing roughly 80% of Russian banking sector assets), as well as defense-related entities and key government officials;
- All transactions in, provision of financing for, and other dealings in **new debt of longer than 14 days maturity or new equity** of the identified Russia-related entities, and their subsidiaries, now prohibited;
- Exportation, reexportation, sale, or supply—directly or indirectly—from the U.S. (or by a U.S. person, wherever located) of **accounting services, trust and corporate formation services, management and consulting services, or quantum computing services** to any person located in Russia now prohibited;
- All **new investment** by U.S. persons in Russia prohibited; and
- Export Controls: The U.S. also currently prohibits a broad range of U.S.-controlled goods for export, reexport, or transfer to Russia and has designated hundreds of Russian entities to the BIS Entity List.



Russia (Cont'd)

Key Designations

More than 80% of the Russian banking sector, including:

- *Designated in 2022:* Promsvyazbank ("PSB Bank"); Vnesheconombank ("VEB Bank"); VTB Bank; Bank Otkritie; Sovcombank; Novikombank; Sberbank; Alfa Bank (Russia); Transkapitalbank ("TKB"); Moscow Industrial Bank; BM Bank JSC ("Bank of Moscow"); and Rosbank.
- *Designated in 2023:* Credit Bank of Moscow PJSC; Lanta Bank; MTS Bank PJSC; Novosibirsk Social Commercial Bank Levoberezhny; Bank Saint Petersburg PJSC; Bank Primorye; SDM Bank; Public Joint Stock Company Ural Bank for Reconstruction and Development ("UBRD"); Bank Uralsib PJSC; and Bank Zenit PJSC.

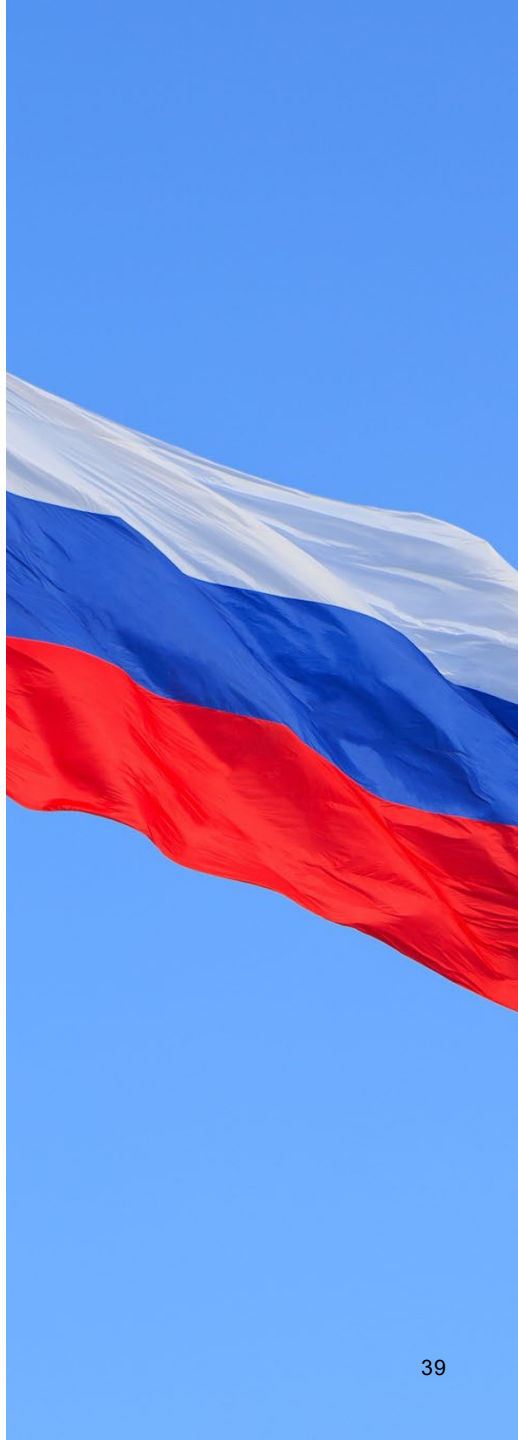
Financial Sector Leaders and Entities, including:

- CEOs and members of executive leadership of VTB Bank, Sberbank, Gazprombank, and the Central Bank of Russia;
- Vladimir Valerievich Komlev (CEO of Russia's National Payment Card System (NSPK)); and
- Leaders of significant Russian financial services entities, including JSC National Settlement Depository, JSC Non-Bank Credit Organization Central Counterparty National Clearing Center, and Russia's Deposit Insurance Agency.

Russian government officials and entities, including:

- Vladimir Putin (Russian President), Sergei Lavrov (Russian Foreign Minister), Sergei Shoigu (Minister of Defense), Valery Gerasimov (Chief of General Staff of the Armed Forces), Dimitry Medvedev, Mikhail Mishustin, other senior Russian officials, and certain of their family members;
- The Russian State Duma and all of its individual members; and
- Federation Council of the Russian Federal assembly and all individual members.

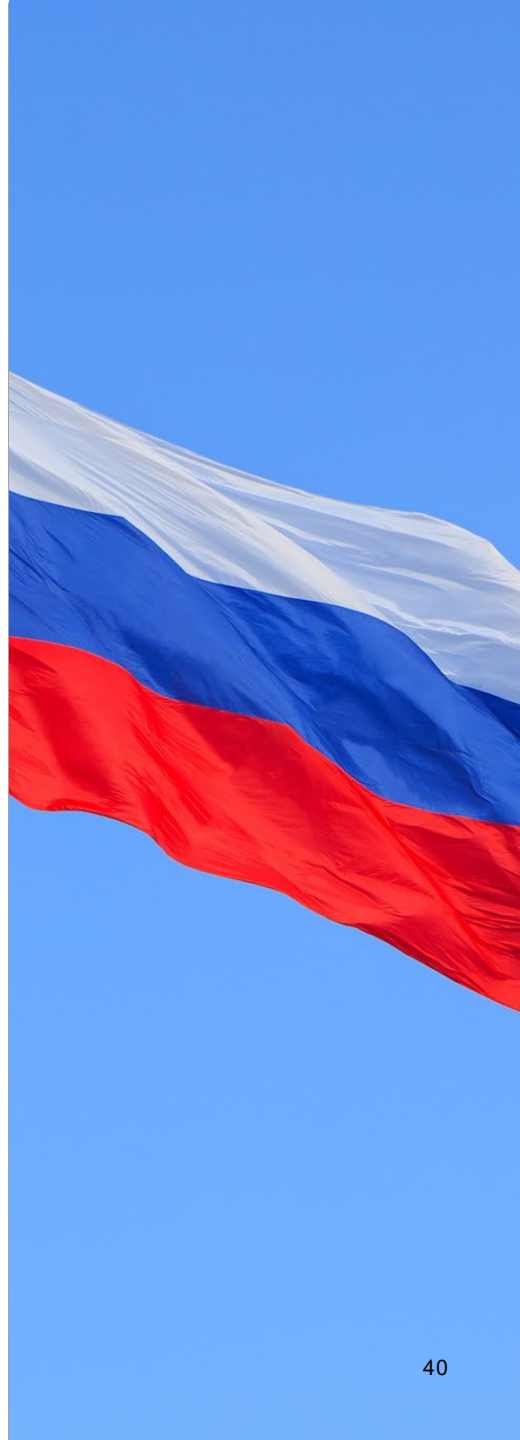
Industrial leaders, oligarchs, and commercial/industrial entities, as well as entities in the energy, mining, media, and virtual currency sectors.



Russia (Cont'd)

Multilateral Price Cap on Russian Crude Oil and Petroleum Products

- Price Cap Coalition includes the G7, Australia, and the European Union.
- Goal is to reduce Russia's overall revenue from oil exports, while maintaining a reliable supply of seaborne Russian oil to the global market and reducing upward pressure on energy prices.
- Prohibits providing many services for Russian oil and petroleum products exported by sea unless the products were purchased below the price cap, including **financing, trading/commodities brokering, insurance, customs brokering, shipping, and flagging.**
  - But, affords **safe harbor** from enforcement for actors retaining either:
    - documentation of **price and "ancillary cost information"** (shipping, freight, and insurance costs); or, if accessing price and ancillary cost information is **impracticable,**
    - attestations to price cap compliance (reinsurers may use sanctions exclusion clauses).
- The price cap is currently set at:
  - $60/barrel price cap on Russian-origin crude oil (effective Dec. 5, 2022);
  - $45/barrel price cap for Russian-origin Discount to Crude petroleum products and $100/barrel cap for Premium to Crude petroleum products (effective Feb. 5, 2023).
- **Enforcement actions, 2023:** October 12, November 16, and December 1. So far, OFAC has designated 6 UAE entities, 1 Turkish entity, and 1 Liberian entity for price cap noncompliance.

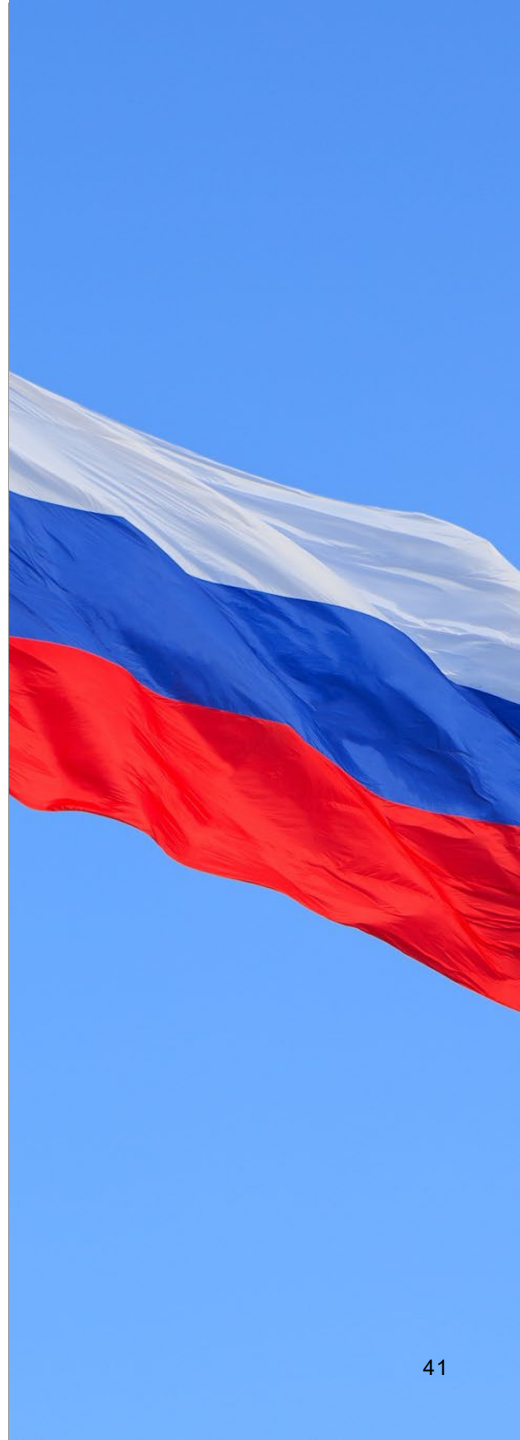


Russia (Cont'd)

New "Exit Tax" Guidance and the Difficulties of Divestment

On February 24, 2023, OFAC released new guidance clarifying that persons subject to U.S. jurisdiction would be required to obtain a specific license prior to paying the Russian "exit tax."

- Because paying the Russian "exit tax" may require transactions involving the Central Bank of Russia and the Ministry of Finance of Russia – which are both subject to Directive 4 – persons subject to U.S. jurisdictions are prohibited under U.S. law from paying the tax, absent a general or specific license.
- Following the implementation of the Russian "exit tax" in December 2022, some relied on General License 13D, which authorized payment of taxes to the Central Bank of Russia and the Ministry of Finance if "ordinarily incident and necessary to such persons' day-to-day operations in the Russian Federation."
- However, OFAC's new guidance clarified that paying the exit tax does not fall within the scope of GL 13D (now GL 13F) because the exit tax is not ordinarily incident or necessary to a person's day-to-day operations, and persons subject to U.S. jurisdictions are required to obtain a specific license from OFAC prior to paying the "exit tax" to the Russian government.
- New guidance complicates efforts of U.S. companies seeking to divest from their Russian businesses.

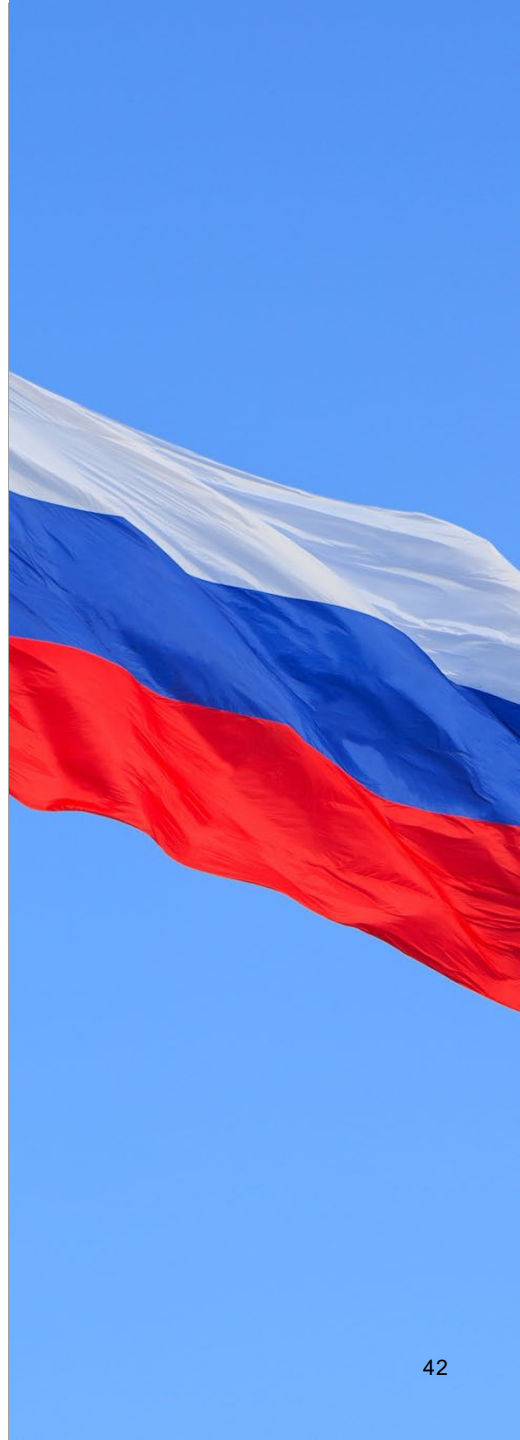


Russia (Cont'd)

On December 22, 2023, the Biden Administration issued a new Executive Order, E.O. 14114, amending E.O. 14024 to authorize OFAC to impose secondary sanctions on foreign financial institutions if they conduct or facilitate:

- significant transactions with persons designated as SDNs within the Russian technology, defense and related materiel, construction, aerospace, and manufacturing sectors;
- significant transactions and services involving sanctioned *or unsanctioned* persons operating in these sectors more broadly; or
- significant transactions with any person *facilitating* the sale, supply, or transfer to Russia of *certain covered items* (e.g., certain machine tools, semiconductor manufacturing equipment, electronic test equipment, advanced optical systems, and navigation instruments).

- *Strict liability* standard.
- OFAC has significant discretion in determining whether a transaction is "significant."
- (iii) in effect imposes a broad export control compliance framework; not limited by existing U.S. export control regulations or product classifications.
- Use of non-USD currency *does not* mitigate sanctions risks.
- A foreign bank processing a significant transaction *in a non-USD currency on behalf of a non-U.S. customer supplying a wholly foreign-produced covered item to Russia* faces sanctions risks under EO 14114.



Russia – EO 14114

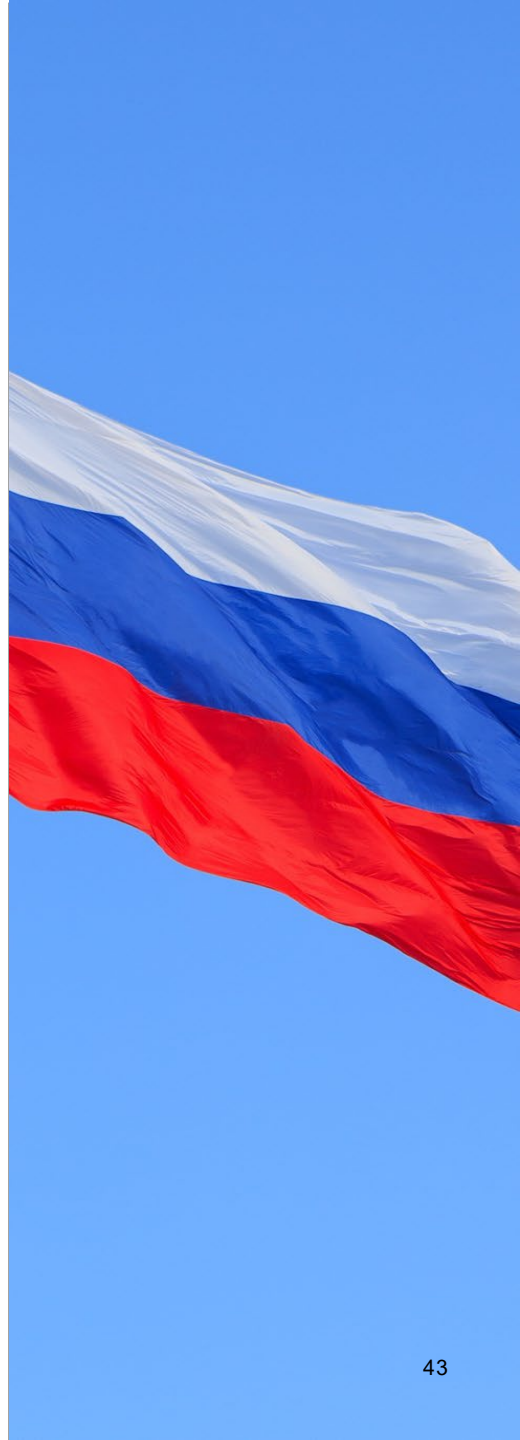
Consequences

For financial institutions deemed to have engaged in EO 14114 sanctionable conduct, OFAC can:

- impose blocking sanctions; or
- prohibit opening or impose strict conditions on maintaining correspondent accounts or payable-through accounts in the U.S.

Considerations

- EO 14114 creates additional due diligence considerations and increased compliance and operational risks for foreign banks when engaging in Russia-related transactions.
- Banks weighing EO 14114 sanctions risks may want to evaluate Russia-related transactions for connections to Russia's military-industrial base or trade in covered items.
- Mitigating such risks may require more nuanced controls – and hence more resources – in order to apply an appropriately risk-tailored program.
- OFAC has issued guidance on identifying EO 14114 sanctions risks and implementing corresponding controls.



Venezuela

Sanctions relief: Oil & Gas, Gold, and Securities

On October 18, 2023, in response to an electoral roadmap agreement between Venezuela's Unitary Platform and representatives of Maduro, OFAC issued four General Licenses suspending select sanctions. On February 2, 2024, in response to developments in Venezuela, OFAC issued an FAQ narrowing the scope of the relief it issued

- Represents significant shift from Trump-era "maximum pressure" campaign that since 2019 had prohibited virtually all U.S. nexus dealings involving key sectors of Venezuela's energy-driven economy.
- OFAC reserved the right to revoke or amend existing licenses at any time if the Maduro regime reneges on its commitments under the electoral agreement, which include allowing a competitive, internationally monitored presidential election next year.

Oil & Gas Sector:

- General License (GL) 44: authorizes U.S. persons, until April 18, 2024, to engage in all transactions related to oil or gas sector operations in Venezuela, including transactions involving state-owned oil giant ***Petróleos de Venezuela, S.A. ("PdVSA"),*** subject to certain conditions. U.S. government announced that it will not be renewed.
- Marks the most substantial easing of U.S. sanctions on Venezuela to date.

Gold Sector:

- General License (GL) 43: authorized most U.S. nexus transactions involving Venezuela's state-owned gold mining company, CVG Compania General de Mineria de Venezuela CA ***("Minerven")***, and its majority-owned entities. This was rescinded.

Government of Venezuela and PdVSA Securities

- The October 2023 measures also removed the secondary trading ban on certain Venezuelan sovereign bonds and PdVSA debt and equity. The ban on trading in the primary Venezuelan bond market remains in place.

Iran

U.S. Gov't Targets Iran Missile Program as UN Sanctions Measures Expire

On October 18, 2023, sanctions targeting Iran under UN Security Council Resolution 2231 expired pursuant to a "sunset" clause of the 2015 Iran nuclear deal. That same day, the U.S. Government took the following actions:

- The U.S. Government, alongside 46 other countries endorsing the Proliferation Security Initiative (PSI), issued a joint statement affirming their commitment to, among other things, "(1) undertake effective measures to interdict the transfer to and from Iran of missile-related materials, including those related to UAVs; (2) adopt streamlined procedures for rapid exchange of relevant information concerning Iran's proliferation activities; (3) review and work to strengthen our relevant national legal authorities to address Iranian missile- and UAV-related issues; and (4) take specific actions in support of interdiction efforts related to Iran's missile and UAV programs."
- The U.S. Department of the Treasury designated 11 individuals, eight entities, and one vessel based in Iran, Hong Kong, China, and Venezuela, each of which were alleged to have enabled Iran's destabilizing ballistic missile and/or unmanned aerial vehicle (UAV) programs.
- The U.S. Departments of the Treasury, Commerce, State, and Justice issued a joint "Iran Ballistic Missile Procurement Advisory," to alert persons and businesses globally to Iran's ballistic missile procurement activities. The Advisory, among other things, describes the deceptive techniques used to further these activities (e.g., obscuring of end-users through transaction layering, false documentation); identifies the persons, entities, and types of goods that have been historically involved in the activities; and discusses ways to minimize risk under applicable sanctions and export control laws. Notably, the Advisory highlights recent DOJ enforcement of Iran-related sanctions and export control violations, as well as DOJ-led initiatives to undermine Iran's ability to acquire missile and other sensitive technology.

The OCC Flags Sanctions Compliance Risk

The Office of the Comptroller of the Currency's Fall 2023 Semi-Annual Risk Perspective continued its focus on identifying elevated sanctions compliance risks that financial institutions should be aware of, including:

"Potential investments in the U.S. commercial real estate sector by sanctioned Russian elites, oligarchs, their family members, and the entities through which they act."

"The heightened geopolitical risks that "could rapidly change the outlook, especially…Russia's invasion of Ukraine [and] increasing U.S. tensions with China."

U.S. Controls on Outbound Investment

"**. . . the United States now is undertaking a period of historic investment in our infrastructure, in our people, in our manufacturing, and in our supply chain. And as a result, we have a very strong economy.**

However, it is not intended to hinder China's economic progress. We believe a strong Chinese economy is a good thing. And President Biden has been crystal clear repeatedly on this point; we seek healthy competition with China. A growing Chinese economy that plays by the rules is in both of our interests. That said, we have to make sure there is a level playing field and we will at all times do what we need to do to protect our workers."

U.S. Secretary of Commerce Gina M. Raimondo, August 28, 2023

U.S. Controls on Outbound Investment: Executive Action

GIBSON DUNN

The Restrictions

- On August 9, 2023, the Biden Administration issued an **Executive Order outlining controls on outbound U.S. investments in certain Chinese entities**, accompanied by an Advance Notice of Proposed Rulemaking ("ANPRM") for public comment.
- **No immediate new legal obligations or restrictions** were imposed.
- In broad strokes, the program will:
- **Prohibit U.S. persons from directly or indirectly entering into certain types of transactions with a covered foreign person** engaged in activities involving the specified covered national security technologies and products; and
- **Require notification to Treasury by U.S. persons** who directly or indirectly enter into the same types of transactions for a broader set of defined covered national security technologies and products.
- Initial target sectors include:
- **Semiconductors and Microelectronics**;
- **Quantum Information Technologies**; and
- **Artificial Intelligence ("AI") Systems**.
- Countries of concern identified as the **People's Republic of China**, including the Special Administrative Regions of **Hong Kong** and **Macau**.

The Implementation Process

- **No effective date** set as of yet and no clear timeline for implementation.
- The ANPRM included a broad list of **83 specific questions** that Treasury posed to the public for comment. Comments were due on September 28, 2023.
- At some undefined point after public comments are received and digested, Treasury will issue a **Notice of Proposed Rulemaking** setting out a draft of the regulations and allowing for public comment.
- The actual rules will come into effect at some point after that public comment period ends, which is **very likely months away**.
- **Allied countries are likely to develop similar restrictions.**
- A G7 statement on May 20, 2023, acknowledged that "appropriate measures designed to address risks from **outbound investment could be important to complement existing tools**."
- The European Commission listed outbound investment as a priority for 2023.
- In May 2023 at the U.S.-EU Trade & Tech Council, the parties agreed to **coordinate any such outbound investment policies**.

U.S. Controls on Outbound Investment: Potential Restrictions from Congress

The Restrictions

- **Cornyn-Casey Outbound Investment Transparency Act**
- Included as part of the Senate's version of the **FY 2024 National Defense Authorization Act**.
- Would require U.S. firms to notify Treasury about investments in covered sectors, such as **semiconductors, AI, quantum technology, hypersonics, satellites, and lasers** in countries of concern—China, Russia, Iran, North Korea.
- Notification regime only, but **includes more sectors and countries of concern** than the Biden Administration's E.O. and ANPRM.
- **House Financial Services Committee Chairman Patrick McHenry** wrote Treasury Secretary Yellen opposing the Administration's outbound investment proposal.
- Questioned the legality of the ANPRM's use of IEEPA as its statutory authority.
- Requested that Treasury re-issue the ANPRM under OFAC or another appropriate office.
- Questioned the value of a regime intended to decrease investment in China.
- Argued that the program's concerns are already covered by existing intellectual property protections, inbound investment screening, and export control regimes.

The Implementation Process

- Cornyn-Casey Outbound Investment Transparency Act may **yet make it into the final NDAA**.
- The act **faces headwinds from key players in both parties**:
- Some argue that **tougher measures** are needed;
- Others claim that such measures would **be ineffective at best** and advantageous to China at worst.
- The **legislative fate of Congressional restrictions remains to be seen** in light of the actions taken by the White House.
- Additional action by Congress in this space **cannot be wholly discounted and may indeed be compatible** with the Biden Administration's proposed regulations.

Newly Imposed Sanctions Involving Actors in Middle East

Since October, OFAC has imposed a number of new sanctions on key actors in the Middle East.

- On October 18, 2023, OFAC levied sanctions on ten Hamas terrorist group members and operatives, as well as select Hamas financiers, following the attacks in Gaza. The sanctions targeted financial supporters located in Sudan, Turkey, Algeria and Qatar.
  - As stated by Treasury officials, the sanctions are an attempt to halt Hamas's funding and cut off their revenue sources, with these names added to over 1,000 other sanctioned persons and entitles with ties to Hamas's terrorism efforts in the Middle East.
- Furthermore, on December 28, 2023, OFAC also imposed sanctions on an individual and Iranian entities responsible for financing Houthi forces—which have been attacking trade and shipping routes in the Red Sea and Gulf of Aden.
  - The sanctions (levied on three entities and one individual) are primarily directed at Iranian institutions that have overseen the flow of Iranian funds to Houthi-backed forces.
  - The sanctions also apply to the head of the Currency Exchangers Association, Nabil Al-Hadha, who serves as a financial intermediary remitting funds to Houthi-forces in the Houthi-controlled area of Sanaa.
- On January 25, 2024, U.S. officials sanctioned four senior members of the Houthi group for further sanctions.

Newly Imposed Sanctions Involving Actors in Middle East (cont'd)

Since October, OFAC has imposed a number of new sanctions on individuals and entities in the Middle East.

- On January 29, 2024, OFAC imposed sanctions on a group of individuals who targeted Iranian dissidents and/or groups opposed to the current Iranian regime.
  - These individuals purportedly murder political opponents at the direction of Iran's Ministry of Intelligence and Security and are led by Naji Ibrahim Sharifi-Zinhashti (an Iranian narcotics trafficker).
  - These individuals remain committed to silencing Iran's perceived critics and have been known to plot operations in the United States as well.
- Additionally, on February 1, 2024, the White House (in conjunction with the Departments of Treasury and State) issued an executive order authorizing the blocking of property, and any interests in property, of any foreign person determined by the Secretary of State to have, among other things, threatened the peace, security, or stability of the West Bank.
  - The order signals a growing effort to thwart violence in the region as the conflict between Israel and Hamas continues.

ENFORCEMENT ACTIONS

03

ENFORCEMENT ACTIONS: DIGITAL ASSET BUSINESSES

Binance

DOJ
FinCEN
OFAC
CFTC

In November 2023, Binance entered into a $4.316 billion resolution with DOJ, FinCEN, OFAC, and the CFTC for alleged failures to register with U.S. regulators, comply with relevant AML and commodities laws, as well as for processing transactions in violation of U.S. sanctions laws.

- Although Binance is a non-U.S. company, U.S. enforcers alleged that because it had U.S. users for a period of time, it was subject to various U.S. laws.
- **BSA Failure to Register**: Under the Bank Secrecy Act, a foreign-located money services business is required to register with FinCEN if it conducts business "wholly or in substantial part within the United States." 31 C.F.R. § 1010.100(ff). DOJ and FinCEN alleged that, on account of the historical U.S. users on the platform, Binance should have registered as a money transmitter.
- **Failure to Maintain an Adequate AML Program**: Similarly, because Binance was allegedly required to register as a money transmitter, it was also required to have an effective AML program under the BSA. DOJ and FinCEN alleged that Binance's AML program was deficient because it did not, for instance, historically conduct full KYC on all users or file SARs with FinCEN.
- **U.S. Economic Sanctions Violations**: DOJ and OFAC also alleged violations of U.S. sanctions laws because Binance's software automatically matched trades between U.S. users on the platform and persons in comprehensively sanctioned jurisdictions, such as Iran.
- **CFTC**: The CFTC also alleged a number of violations, including illegally offering and executing commodity derivatives transactions and willful violation of the Commodities Exchange Act.

Binance (Cont'd)

DOJ
FinCEN
OFAC
CFTC

Some notable aspects of this resolution include:

- **Cooperation Credit:** Although Binance did not receive voluntary self-disclosure credit, it received partial cooperation and agreed to a criminal fine which reflected a 20% discount off of the bottom of the applicable Sentencing Guidelines.
- **Scope:** The DOJ agreement binds the Criminal and National Security Divisions of DOJ, along with the U.S. Attorney's Office for the Western District of Washington. Under the terms of the FinCEN and CFTC resolutions, Binance admitted only to the facts in the DOJ plea agreement. Similarly, the OFAC resolution contained language that the agreement was not an admission by the company of alleged violations.
- **Compliance and Reporting Obligations:** Binance agreed to report any knowledge of certain potential violations of law and otherwise cooperate with DOJ and other agencies. Binance also made and committed to maintain various compliance commitments pertaining largely to AML controls.
- **Monitor**: Under the terms of the resolution, Binance agreed with DOJ, FinCEN, and OFAC to have an independent compliance monitor. This is the first time FinCEN is responsible for selecting and overseeing a compliance monitor.

CoinList

OFAC

CoinList Markets LLC ("CoinList") (December 2023): CoinList agreed to pay $1,207,830 to settle its potential civil liability arising from processing 989 transactions on behalf of users ordinarily resident in Crimea between April 2020 and May 2022, in apparent violation of OFAC's Russia/Ukraine sanctions.

- CoinList, a virtual currency exchange, maintained several sanctions compliance measures during the relevant period. Nonetheless, these screening procedures allegedly failed to capture users who represented themselves as residents of a non-embargoed country but who provided an address within Crimea. In particular, CoinList opened 89 accounts for customers, nearly all of whom had specified "Russia" as their country of residence but all of whom provided addresses in Crimea upon account opening.

OFAC identified the companies' cooperation with the investigation, the relatively small volume of the transactions, and remedial measures as mitigating factors.

- Due in part to CoinList's financial condition, $300,000 of the settlement amount was suspended pending CoinList's satisfactory completion of specific compliance commitments.
- CoinList also agreed to invest $300,000 in additional sanctions compliance controls, including with respect to enhanced screening controls and additional compliance staff.

OFAC

- In August 2022, OFAC designated virtual currency mixer, Tornado Cash, a decentralized, smart contract mixer, operated by self-executing code running on the Ethereum blockchain.
    - Tornado Cash was initially designated under E.O. 13694 (targeting malicious cyber activity) and later designated under E.O. 13722 (targeting North Korea).
- Six blockchain users challenged OFAC's designation of Tornado Cash in the Western District of Texas. In August 2023, the district court rejected plaintiffs' claims, ruling that Treasury was within its statutory authority to designate Tornado Cash and that it was appropriate for Treasury to consider Tornado Cash a "person" rather than simply an autonomous software. The decision has been appealed.
- Also in August 2023, DOJ charged Tornado Cash founders Roman Storm and Roman Semenov with conspiracy to commit money laundering, conspiracy to commit sanctions violations, and conspiracy to operate an unlicensed money transmitting business, all arising out of their' alleged creation, operation, and promotion of Tornado Cash.

Nathaniel Chastain (OpenSea)

DOJ

- According to DOJ, from June 2021 to September 2021, Chastain purchased NFTs knowing they would soon be featured on OpenSea's homepage, and once they were featured on the homepage, Chastain sold the NFTs at 2-5x the initial purchase price. DOJ alleged that Chastain conducted the trades using anonymous digital currency wallets and accounts on OpenSea.
- On May 3, 2023, a jury found Chastain guilty of wire fraud and money laundering, and on August 22, 2023, he was sentenced to three months of home confinement, three years of supervised release, a $50,000 fine, and forfeiture of the Ethereum he made trading the featured NFTs.
- In June 2022, DOJ unsealed an indictment charging Nathaniel Chastain, a former product manager of OpenSea with wire fraud and money laundering in connection with an alleged scheme to commit insider trading in NFTs using confidential information about what NFTs were going to be featured on OpenSea's homepage.

Sam Bankman-Fried (FTX)

DOJ

- Last year, DOJ unsealed a superseding indictment replacing a December 2022 one charging Sam Bankman-Fried, FTX Founder and CEO, with money laundering, operating an unlicensed money transmission business, and bank fraud in addition to several wire fraud and unlawful political donations charges.
- Indictment alleges Bankman-Fried used bank accounts in the names of Alameda Research and North Dimension in order to accept FTX customer funds and engage in transmission with those funds after the bank indicated FTX would need to be registered as a money transmitter and undergo extensive diligence in order to itself open an account for that purpose.
- DOJ further alleges that North Dimension was created by Bankman-Fried to open a bank account that could be used for FTX purposes and that Bankman-Fried falsely indicated in bank documents that North Dimension was not a money transmitter, resulting in less onboarding diligence.
- Bankman-Fried was found guilty of all charges.

Bitpay

NYDFS

- **March 2023 Consent Order and $1 million penalty against Bitpay for BSA/AML program and sanctions screening deficiencies, failure to conduct periodic cybersecurity risk assessments, and failure to appoint a CISO.**
- DFS highlighted the below findings:
  - Insufficient independent testing of its transaction monitoring system
  - Lack of quality assurance processes for OFAC screening
  - Ad hoc application of customer risk rating processes
  - Siloed onboarding processes and systems
  - Lack of policies and procedures governing rule management, QA and risk assessments.

Coinbase

NYDFS

- In January 2023, cryptocurrency exchange Coinbase entered into a $100 million settlement with the New York Department of Financial Services ("DFS") based on "significant failures" in Coinbase's AML compliance program.
  - The settlement amount included a $50 million penalty and $50 million towards compliance enhancements.
  - The resolution documents described the following alleged deficiencies underlying the settlement:
  - KYC/CDD program was "immature and inadequate" and treated onboarding requirements as a "check-the-box exercise" without conducting appropriate due diligence;
  - Compliance function did not grow commensurate with its growth; and
  - Transaction monitoring backlogs caused missed regulatory deadlines for investigating, reporting, and remediating suspicious activity.
- In the course of its investigation, in 2022, DFS installed an independent compliance monitor to work with Coinbase on compliance enhancements, and its consent order requires Coinbase to continue to work with the monitor for at least one additional year, extendable at DFS's discretion.

ENFORCEMENT ACTIONS: CIP/CDD AND TRANSACTION MONITORING PROCESSES

Shinhan Bank America

FinCEN

On September 29, 2023, FinCEN assessed a $15 million civil penalty against Shinhan Bank America for willful violation of the BSA. The Consent Order includes the first detailed discussion by FinCEN of the risk rating expectations under the AML Program CDD Rules. It also is part of a recent pattern of statements reflecting a particular focus on, and increasingly sophisticated expectations for, customer due diligence and transaction monitoring systems.

- Banks should maintain formal customer risk rating procedures that establish a baseline risk rating score at onboarding that is periodically updated over the course of a customer relationship based on changes in the customer's activity at the financial institution or other new information learned about the customer.
- Risk ratings should be per customer, not per product, and therefore, should be based on a customer's activity across all accounts with the bank.
- Procedures for customer risk ratings should be sufficiently nuanced to distinguish customers that present materially different risks. FinCEN criticized Shinhan's overly "rigid" methodology for calculating customer risk rating scores. Accordingly, risk ratings should not solely be based on the type of customer (e.g., entity vs. individual, or U.S. resident vs. foreign resident) or the type of product (e.g., business vs. personal account, or checking vs. savings account). Rather, they should be sufficiently nuanced to distinguish between materially different risks posed by customers in each of those categories.
- Institutions must have CDD procedures for understanding the nature and purpose of customer relationships in order to develop these risk profiles.

Shinhan Bank America (Cont'd)

FinCEN

Transaction Monitoring

- Customer's risk rating should inform the transaction monitoring scenarios applied to that relationship.
- FinCEN and other regulators have been increasingly indicating that they expect that institutions will have automatic transaction monitoring systems that are regularly and comprehensively tested to make sure all scenarios alert as intended, all relevant data properly feeds into the system, scenarios are sufficient and tailored for each product, and scenarios are appropriately applied to ingested data. There has similarly been an emphasis on regularly updated and sufficiently comprehensive transaction monitoring scenarios that are both rules-based and behavior-based.
- The Shinhan decision includes several examples of scenarios that should be incorporated within a transaction monitoring system that should be checked against a bank's current system:
    - Scenarios for wire transfers sent to several beneficiaries from a single originator, or sent from several originators to a single beneficiary;
    - Scenarios for transactions passing through a large number of jurisdictions;
    - Scenarios for transactions conducted using Remote Deposit Capture;
    - Scenarios involving a series of transactions involving different types of activity (i.e., check deposit followed by a wire transaction, or a wire transaction followed by an ACH); and
    - Scenarios that apply to account-specific customer activity and clustered activity across all of a customer's accounts.

Shinhan Bank America (Cont'd)

NYDFS
FDIC

- FDIC also announced a $5 million penalty for the same BSA/AML program violations and for failing to comply with a prior FDIC Consent Order regarding BSA/AML program deficiencies. FDIC credited the $15 million penalty to FinCEN as satisfying its penalty.
- Shinhan also entered into a $10 million settlement wit NYDFS for failing to maintain an effective and compliance BSA/AML program and incorrectly certifying Part 504 compliance with the Department.
    - NYDFS highlighted that Shinhan failed to adequately remediate its BSA/AML program deficiencies despite two prior FDIC Consent Orders and a Memorandum of Understanding with NYDFS for the same issue.
    - NYDFS also required Shinhan to submit a detailed remediation action plan that was subject to the Department's approval.

Bancredito International Bank and Trust Corporation

FinCEN

On September 15, 2023, FinCEN announced a Consent Order and $15 million civil penalty against Bancredito International Bank and Trust Corporation as the first enforcement action under FinCEN's "gap rule" for banks without a federal functional regulator. The Order is based on willful failures to implement and maintain an adequate BSA/AML Program, establish an adequate due diligence program for correspondent accounts for foreign financial institutions, and timely and adequately file suspicious activity reports.

- Bancredito's local regulator in Puerto Rico had repeatedly found BSA/AML deficiencies at the bank during exams dating back to 2012, which the bank did not adequately remediate.
- Per the facts in the Consent Order, the bank lacked basic BSA/AML processes, failed to file any SAR for a number of years despite a significant volume of high-risk customers, and had a culture of BSA noncompliance.
- Bancredito surrendered its banking license as part of the resolution and agreed not to obtain any new banking license.

Kingdom Trust Company

FinCEN

On April 26, 2023, FinCEN assessed a $1.5 million civil penalty against South Dakota-chartered Kingdom Trust Company for willful violation of the BSA, representing FinCEN's first enforcement action against a trust company.

- Kingdom Trust opened accounts and provided services for Latin America-based trading companies and financial institutions with virtually no controls to identify or assess suspicious transactions.
- Kingdom Trust maintains operational headquarters in Kentucky and was in the business of providing custodial services to individual investors and investment advisors.
- Through a consultant, Kingdom Trust was referred clients based in Uruguay, Argentina, Panama, and other locations for the purpose of opening accounts, holding cash and securities, and facilitating payments for the benefit of these customers.
- The customers initiated a high volume of suspicious transactions (~$4 bn) that went unchecked and unreported by Kingdom Trust. At the time, Kingdom Trust's AML compliance consisted of a single individual responsible for manually reviewing daily transactions. Some customers were the subject of prior media reports related to money laundering and securities fraud.
- FinCEN found that Kingdom Trust willfully failed to accurately and timely report suspicious transactions in violation of the BSA and required the company to conduct a lookback and independent AML program audit.

Deutsche Bank

FED

In July 2023, the Fed announced a Consent Order and $186M fine against Deutsche Bank arising from the alleged insufficient remedial progress under prior consent orders to enhance the bank's BSA/AML and sanctions programs. In particular, the Consent Order focused on the bank's need to:

- Improve systems and data supporting the AML transaction monitoring program and OFAC transaction filtering processes, including by ensuring the lack of system gaps through Data Trace Analyses;
- Implementation of a comprehensive CDD Program particularly for medium- and high-risk customers; and
- Creation of a transaction monitoring framework that is risk-based, has scenarios that function as intended and includes effective alert investigation processes.

Gyanendra Kumar Asre

FinCEN DOJ

In January 2024, FinCEN and DOJ announced an enforcement action and plea agreement, respectively, against Gyanendra Kumar Asre for violations of the Bank Secrecy Act.

- Asre, a longtime participant in the financial services industry, served as a director of the New York State Employees' Federal Credit Union (NYSEFCU) and as Chairman and CEO of DDH Group LLC (DDH), an MSB.
- The crux of FinCEN and DOJ's focus involved Asre's transformation of NYSEFCU into a conduit for repatriating large sums of cash and checks from Mexico through MSBs that Asre himself controlled (such as DDH).
- In making these changes to NYSEFCU's financial profile, Asre failed to comply with several important BSA requirements necessary for NYSEFCU's ability to successfully facilitate these transactions without inviting unnecessary risk. These included:
    - Asre's failure to register DDH, as an MSB, with FinCEN;
    - Asre's failure to develop and maintain an effective AML program for the NYSEFCU, which included the following: (1) not developing a system that could detect and report suspicious transactions; (2) not establishing a Customer Identification Program or appropriate Customer Due Diligence mechanisms to confirm that NYSEFCU's new MSB customers were registered with FinCEN or in good standing under relevant state laws; and (3) failure to screen DDH's account activity against the OFAC Specially Designated Nationals and Blocked Persons List to determine if its customers were subject to sanctions restrictions.
- As a result of these failures, hundreds of millions of dollars in high-risk and suspicious funds moved through the NYSEFCU without proper monitoring or reporting to FinCEN. Due to these reporting failures, Asre must now pay $100,000 in civil monetary penalties.
- Alongside FinCEN's enforcement efforts, the DOJ's Money Laundering and Asset Recovery Section (MLARS) brought charges against Asre in a parallel proceeding for criminal violations of the BSA. In January 2024, Asre has entered a guilty plea related to those charges as well.

City National Bank

OCC

- **In January 2024, the OCC announced a Consent Order and $65 million civil money penalty against City National Bank in connection with findings that the bank engaged in unsafe and unsound practices and BSA violations.**
- The Consent Order required the bank to take a number of remedial undertakings to enhance its BSA/AML and Sanctions compliance program, including:
  - Implementing BSA/AML internal controls, including updated transaction monitoring thresholds that are periodically tested and monitored, approved by senior management and reported to the Board, and independently validated.
  - Procedures to ensure there is sufficient personnel to satisfy SAR filing requirements and that they have adequate expertise, training, authority, and resources to fulfill that function,
  - Detailed methodologies for performing at least annual BSA/AML and sanctions risk assessments.
  - CDD procedures that include a methodology for risk rating customers, adverse media screening on all new customers, collection of sufficient information at onboarding to inform risk ratings and suspicious activity monitoring, and ongoing, periodic reviews of high-risk customers.
    - Risk levels should take into consideration the customer's entire relationship, customer type, account purpose, expected account activity, and geographic location.

American Express National Bank

OCC

- **In July 2023, the OCC issued a Consent Order and $15M civil penalty against American Express National Bank for CIP and recordkeeping violations based on alleged failures to:**
  - Obtain EINs for certain customers;
  - Maintain records regarding CIP compliance;
  - Maintain records regarding efforts to retain certain customers and produce such records to the OCC; and
  - Properly govern and oversee a third-party affiliate that assisted with obtaining customers for the bank.

ENFORCEMENT ACTIONS: FINTECHS AND PAYMENT SOLUTIONS

NASDAQ

OFAC

Nasdaq, Inc. (December 2023): The U.S.-based financial services company Nasdaq entered into an approximately $4 million settlement with OFAC involving alleged Iran-related conduct by a former subsidiary organized in Armenia.

- Conduct at issue involved an indirect subsidiary, Nasdaq OMX Armenia OJSC, that formerly owned and operated the Armenian Stock Exchange (ASE).
- Company operated ASE trading platforms that, pursuant to Armenian law, provided Armenian banks access to overnight liquidity loans and foreign exchange.
- From 2012 to 2014, Nasdaq OMX Armenia allegedly processed trades and settled payments through the ASE platform involving the OFAC-designated Armenian subsidiary of Iran's state-owned Bank Mellat.
- OFAC alleged that Nasdaq OMX Armenia knowingly engaged in the exportation of services to Iran and the Government of Iran, thereby committing 151 apparent violations of the Iranian Transactions and Sanctions Regulations (ITSR).
- Conduct was voluntarily self-disclosed to OFAC and Nasdaq OMX Armenia earned approximately $16,000 in commissions and fees over the relevant period from processing the transactions at issue.
- OFAC cited as an aggravating factor Nasdaq and Nasdaq OMX Armenia's "actual knowledge" that Mellat Armenia was trading on the ASE after Nasdaq OMX Armenia became subject to the ITSR in 2012.
- OFAC identified numerous mitigating factors, including Nasdaq's full cooperation with the agency's investigation and extensive remedial measures such as divesting the foreign subsidiary at issue.

Wells Fargo

OFAC
FED

On March 30, 2023, OFAC announced a $30,000,000 settlement with Wells Fargo Bank, N.A. ("Wells Fargo") for providing software to a foreign bank that was allegedly used to process trade finance transactions in violation of U.S. sanctions targeting Iran, Syria, and Sudan.

- OFAC alleged that Wells Fargo's predecessor, Wachovia Bank ("Wachovia"), developed a trade insourcing software platform for general use by a European Bank, which the foreign bank then used to manage transactions involving sanctioned jurisdictions and persons. According to OFAC, Wells Fargo did not identify or stop this use for seven years despite potential concerns raised internally within Wells Fargo on multiple occasions following Wells Fargo's acquisition of Wachovia. The apparent violations were voluntarily self-disclosed.
- Aggravating factors included (but were not limited to): (1) "reckless disregard" for U.S. sanctions requirements by Wachovia's legacy Global Trade Services ("GTS") Unit, which developed the software; (2) Wells Fargo should have known the software was being used for transactions involving sanctioned persons; and (3) Wells Fargo and Wachovia were large and sophisticated financial institutions.
- Mitigating factors included (but were not limited to): (1) the legacy GTS unit was relatively small, and there was no indication the conduct was directed by senior management or the result of a systemic compliance breakdown; (2) the majority of the apparent violations related to agriculture, medicine, and telecommunications and may have been eligible for a general or specific license; and (3) Wells Fargo took appropriate investigative and remedial steps.

That same day, the Federal Reserve Board announced in parallel a $67,762,500 settlement withholding company Wells Fargo & Company for inadequate oversight of sanctions compliance risks with respect to the provision of this software by its subsidiary bank, Wells Fargo.

daVinci Payments

OFAC

Swift Prepaid Solutions, Inc. d/b/a daVinci Payments ("daVinci") (November 2023): daVinci, a financial services and payments firm agreed to remit $206,213 to settle its potential civil liability for 12,391 apparent violations of OFAC sanctions on Crimea, Iran, Syria, and Cuba.

- Between March 2020 and February 2022, daVinci discovered that on 12,378 occasions it had redeemed prepaid cards for users with Internet Protocol (IP) addresses associated with Iran, Syria, Cuba, and Crimea.
- The absence of comprehensive geolocation controls led daVinci to process 12,391 redemptions totaling $549,134.89 for cardholders apparently located in sanctioned jurisdictions.

OFAC identified the companies' cooperation with the investigation and significant remedial measures as mitigating factors.

- The significant remedial measures, included proactively conducting an internally initiated review, implementing IP blocking of access to its platform from sanctioned jurisdictions, conducting real-time screening and blocking of email address suffixes, and instituting independent third-party testing at regular intervals.

Metropolitan Commercial Bank

NYDFS Fed

- In October 2023, Metropolitan Commercial Bank ("MCB") entered into a $15 million settlement with NYDFS arising out of alleged BSA/AML program violations in connection with its partnership with fintech MovoCash to offer a prepaid card.
- In addition to the penalty, MCB was required to submit a number of reports to NYDFS, including detailed information about processes for third-party program manager relationships and updates to its BSA/AML program, governance and oversight structures, and CIP processes relating to the MovoCash prepaid product and relationship.
- NYDFS highlighted the following findings:
  - MCB failed to adequately oversee MovoCash's performance of CIP responsibilities on MCB's behalf.
  - MCB continued to allow MovoCash to handle CIP processes despite multiple notices over time that a high volume of fraudulent accounts were being opened and that MovoCash's CIP processes were not functioning properly.
  - MCB did not immediately notify NYDFS upon learning about the ongoing fraud concerns with MovoCash "as is legally required."
- MCB also settled with the Fed with a $14,478,676 civil money penalty for the CIP deficiencies and agreed to CIP, CDD, and third-party risk management program enhancements.

Payoneer

NYDFS

- **November 2023 Consent Order and $1.25 million penalty against Payoneer for OFAC compliance program deficiencies** that contributed to transactions to sanctioned parties in 2013 through 2018.
- DFS highlighted the following deficiencies in controls:
  - "Weak algorithms that allows close matches to SDN List entries to evade Payoneer's sanctions filter"
  - "Failure to screen for Business Identifier Codes even when SDN List entries contained them"
  - "Allowing flagged and pending payments to be automatically released without review during backlog periods"

Privilege Underwriters Reciprocal Exchange

OFAC

Privilege Underwriters Reciprocal Exchange ("PURE") (December 2023): PURE entered into a $466,200 settlement with OFAC for apparent violations of OFAC's Ukraine-/Russia-Related sanctions.

- In 2010, PURE issued a private fleet auto insurance policy, a jewelry and art insurance policy, and two high-value homeowners insurance policies to Medallion, Inc. of Panama, owned by Victor Vekselberg (Vekselberg). The four policies were renewed annually thereafter.
- On April 6, 2018, OFAC added Vekselberg to OFAC's List of SDNs and Blocked Persons pursuant to E.O. 13662. In engaging in 39 transactions totaling $315,891 with a blocked person between May 2018 and July 2020, PURE apparently violated the Ukraine-/Russia-Related Sanctions Regulations. OFAC specifically cited PURE's failure to ensure ownership information about a customer was incorporated into its sanctions screening program as an aggravating factor.

OFAC identified the companies' cooperation with the investigation and remedial measures as mitigating factors.

- PURE cooperated with OFAC's investigation by providing information and timely responses to OFAC. PURE also signed a tolling agreement.
- PURE undertook several remedial measures, including screening its entire customer base through two third-party vendor tools, and requiring its underwriting department to upload all potential or existing customers' corporate disclosure statements into PURE's system.

ENFORCEMENT ACTIONS: USE OF U.S. FINANCIAL SYSTEM BY NON-U.S. ENTITIES

Use of U.S. Financial System by Non-U.S. Entities

OFAC

Over the past two years, OFAC has continued to focus on transactions by non-U.S. entities utilizing the U.S. financial system in violation of various sanctions programs.

- *Sojitz (Hong Kong) Limited (January 2022):* Sojitz (Hong Kong) Limited agreed to pay $5,228,298 for causing U.S. financial institutions to engage in prohibited transactions related to goods of Iranian origin. The relevant transactions involved a Hong Kong-based company, a Thai supplier, and banks in Hong Kong and Thailand. The payments, however, were made in U.S. dollars and involved processing and clearing through U.S. financial institutions, including U.S. corresponding banks of the Hong Kong and Thai banks involved.
- *Danfoss A/S (December 2022):* Danfoss A/S ("Danfoss"), a multinational Danish company that manufactures and sells refrigeration products, air conditioners, compressors, and other cooling products agreed to pay $4,379,810 as a result of its UAE subsidiary causing U.S. financial institutions to engage in prohibited transactions involving Iran, Sudan, and Syria. Employees of Danfoss's UAE subsidiary directed customers in sanctioned jurisdictions to remit payments to U.S. Branch Accounts and used third-party payers in non-sanctioned jurisdictions to disguise the payments. OFAC specifically cited deficiencies in Danfoss's global sanctions compliance program as an aggravating factor.
- *Swedbank Latvia AS (June 2023):* Swedbank Latvia AS ("Swedbank Latvia"), headquartered in Riga, Latvia, and a subsidiary of Swedbank AB, an international financial institution headquartered in Stockholm, Sweden, agreed to pay $3,430,000 to settle liability for allowing its client to initiate payments from Crimea through its e-banking platform that were ultimately processed by a U.S. correspondent bank, even though Swedbank Latvia had reason to know the client was in located in Crimea.

ENFORCEMENT ACTIONS: SANCTIONS SCREENING DEFICIENCIES

Restricted Party Screening

OFAC

Enforcement actions highlight the need for a risk-based approach to sanctioned party screening.

- *MidFirst Bank (July 2022):* OFAC issued a Finding of Violation for maintaining accounts and processing payments on behalf of two SDNs for 14 days post-designation. The vast majority of the value of the transactions occurred within hours of the designations. MidFirst mistakenly believed that its sanction screening vendor screened its entire customer base daily.
- *Tango Card, Inc. (September 2022):* OFAC brought an action against Tango Card for allegedly distributing electronic rewards to individuals with IP and email addresses associated with Cuba, Iran, Syria, North Korea, and Crimea. Tango Card only used geolocation tools and OFAC screening for senders of rewards, and not recipients of awards.
- *Microsoft Corporation (April 2023):* Microsoft agreed to pay $2,980,265.86 to settle more than 1,300 apparent violations of multiple sanctions programs related to the exportation of services and software from the U.S. to comprehensively sanctioned jurisdictions and to SDNs. While Microsoft did have restricted party screening in place, their program did not aggregate information across databases to identify SDNs or blocked persons. Microsoft also failed to timely rescreen and evaluate existing customers following updates to the SDN List, and did not evaluate customers under the 50 Percent Rule.

Restricted Party Screening

OFAC

Emigrant Bank (September 2023): Emigrant Bank entered into a settlement agreement for $31,867.90 to resolve allegations that it had maintained a Certificate of Deposit (CD) account on behalf of two individuals ordinarily resident in Iran, for which it processed 30 transactions between June 2017 and March 2021. According to OFAC, Emigrant Bank, had "actual knowledge of the Iranian address and apparent location of the account holders during this period," having possessed letters and tax forms showing the Iranian address. After the accounts were internally flagged for potential sanctions implications, Emigrant Bank took no remedial action because of an erroneous reliance on an Iran general license authorizing personal remittances.

Industrial and Commercial Bank of China

NYDFS

- In December 2023, NYDFS announced a Consent Order and $30 million penalty against Industrial and Commercial Bank of China for:
  - BSA/AML and sanctions screening program deficiencies that persisted for several years despite a Consent Order from the Fed.
  - Failure to maintain appropriate books and records arising out of certifications that were signed a year later and back-dated due to an internal policy that required the signatures.
  - Failing to immediately notify the Superintendent about the back-dated signatures.
  - Improperly sharing confidential supervisory information with a foreign affiliate without obtaining prior written authorization from the Fed and NYDFS.
- The Fed also brought an enforcement action with $2.4 million fine for the unauthorized use and disclosure of confidential supervisory information.

ENFORCEMENT ACTIONS: DOJ SANCTIONS CASES

Focus on Sanctions Evasion Involving Iran

DOJ has initiated criminal and civil actions designed to stop Iran's illicit crude sales in violation of U.S.-imposed sanctions:

- In the past year, Iran's Islamic Revolutionary Guard Corps (IRGC) and the IRGC-Qods Force (IRGC-QF)—both of which are sanctioned entities and designated Foreign Terrorist Organizations (FTOs)—have allegedly attempted to use the U.S. financial system, including correspondent accounts, to further the illicit sale of crude oil to purportedly fund future terrorist activities.
- In April of 2023, Suez Rajan Limited pleaded guilty to conspiracy to violate U.S. sanctions laws for allegedly disguising the origin of Iranian oil using ship-to-ship transfers, false automatic identification system reporting, falsified documents, and other means. That plea marked the first criminal resolution involving a company that violated sanctions by facilitating the illicit sale and transport of Iranian oil.
- As of September 8, 2023, DOJ announced that the illicit proceeds of that scheme are now subject to a civil forfeiture action, which remains pending in the District of Columbia.
- On February 2, 2024, the DOJ unsealed three additional criminal and civil actions against persons and companies engaged in similar activities:
    - The first action, a criminal prosecution in the Southern District of New York, involves seven defendants charged with terrorism, sanctions evasion, fraud, and money laundering offenses in connection with their trafficking and selling of Iranian oil to government-affiliated buyers in China, Russia, and Syria—all of whom allegedly used correspondent accounts at U.S. financial institutions to facilitate the sales.
    - The second action, a criminal prosecution in the District of Columbia, involved the sale of Iranian oil to Chinese government-owned refineries. The defendants allegedly used shell corporations to launder oil sale proceeds through the U.S. financial system and provided false information to U.S. companies about the source of the transactions.
    - The third action is a civil forfeiture proceeding in the District of Columbia aimed at seizing 500,000 barrels of oil under relevant terrorism laws.

Focus on Sanctions Evasion Involving Select Russian Oligarchs

In 2023, DOJ brought a number of prosecutions against individuals tied to oligarch Viktor Vekselberg for facilitating sanctions evasions:

- In March of 2018, OFAC designated Viktor Vekselberg, a Russian Oligarch, as a Specially Designated National ("SDN")—blocking his assets and preventing his association with U.S. financial markets.
- In 2023, federal prosecutors on DOJ's Task Force KleptoCapture brought several prosecutions against Vekselberg's associates for evading OFAC's imposition of sanctions against Vekselberg.
- First, on January, 20, 2023, DOJ announced the indictment of Vladislav Osipov and Richard Masters for facilitating a sanctions evasion and money laundering scheme related to a 255-foot luxury yacht owned by Vekselberg.
    - Specifically, Osipov and Masters used U.S. companies to manage the operation of the vessel while simultaneously obfuscating Vekselberg's involvement through the use of payments through third parties and non-U.S. currencies to conduct business transactions with U.S. companies
- Next, on February 7, 2023, federal prosecutors announced the indictment of Vladimir Voronchenko, an associate of Vekselberg's, for making more than $4 million in payments to maintain four U.S. properties owned by Vekselberg. These charges also involved an attempt to sell two of those properties.
- Then, on February 24, 2023, prosecutors brought a civil forfeiture complaint against six of Vekselberg's properties in New York City, Southampton, New York, and Fisher Island, Florida—alleging that they were the proceeds of sanctions violations.
- Finally, on April 25, 2023, DOJ initiated prosecutions against Vekselberg's U.S. associates for their role in assisting with Vekselberg's evasion of U.S. sanctions. Specifically, through the use of transfers from a Russian bank account and offshore accounts located in the Bahamas, defendants received 25 wire transfers totaling nearly $3.8 million, all in an effort to circumvent OFAC controls. The funds were used to maintain and service Vekselberg's properties in defiance of U.S. sanctions.

British American Tobacco

In April of 2023, DOJ and OFAC respectively announced criminal and civil fines owed by British American Tobacco for sales in North Korea that violate U.S. sanctions.

- British American Tobacco (BAT) and its subsidiary, BAT Marketing Singapore (BATMS), agreed to pay more than $629 million to resolve bank fraud and sanctions violations stemming from a scheme to conduct business in North Korea through a third-party company in Singapore, all of which violated the federal bank fraud statute and the International Emergency Economic Powers Act (IEEPA).
- BATMS pleaded guilty to conspiracy to commit bank fraud and conspiracy to violate IEEPA while BAT entered into a deferred prosecution agreement in relation to the same charges.
- The decade-long scheme involved BAT and BATMS receiving payments for sales of tobacco to North Korean entities—with payments disguised through correspondent banking transactions that eventually passed to BAT and BATMS through a company incorporated in Singapore, obfuscating the company's connection to North Korea from U.S. officials for a time.
- On the same day as DOJ's announced penalties, OFAC separately entered into a $508 million settlement agreement with BAT involving related conduct—which violated U.S. sanctions on North Korea as proliferators of weapons of mass destruction.
- This settlement is OFAC's largest ever with a non-financial institution and constitutes the maximum statutory penalty capable of being imposed.
- As spelled out by OFAC, the scheme involved North Korean companies remitting profits and payments through BAT's Singapore subsidiary: British-American Tobacco Marketing PTE, Ltd. (BATM). Though BAT did not work directly with sanctioned Korean entities, it was nevertheless liable because it used the U.S. financial system to further the company's infusion of tobacco and cigarette products into blocked North Korean markets.

National Security Division Export Control Prosecutions

In the past year, DOJ's National Security Division (NSD) (through the operation of two new task forces) has prioritized prosecuting corporations and individuals who would seek to undermine national security by evading export controls and sanctions.

- DOJ's Kleptocapture Task Force—created to hold oligarchs accountable for Russia's invasion of Ukraine—has charged more than 40 individuals for engaging in illicit transactions that could support the Russian regime. In one recent case, a president of an Orlando-based company pleaded guilty to acquiring $150 million in products owned by a sanctioned Russian oligarch.
- Additionally, DOJ and the Department of Commerce have collaborated to create the Disruptive Technology Strike Force (DTSF)—a group designed to pursue criminal prosecutions and enforcement actions against persons and companies that export sensitive and/or emerging technologies to sanctioned actors and unfriendly regimes in violation of federal law. Since its creation a year ago, notable DTSF prosecutions include:
    - Actions aimed at Russian procurement networks who received sensitive technologies such has military and airplane equipment from sources in violation of U.S. export laws;
    - Cases charging software engineers with stealing hardware source code from domestic tech companies in order to subsequently market them to Chinese competitors;
    - Prosecution of a Chinese national attempting to sell materials necessary for production of weapons of mass destruction to Iran;
    - Additionally, the DTSF also recently charged cases where sensitive components necessary for military equipment were routed to Russia through intermediaries located in Cyprus, Latvia and Hong Kong.
- These actions demonstrate the effective collaboration of DOJ, Commerce, and Intelligence Community officials in enforcing sanctions and export-control provisions.

ENFORCEMENT ACTIONS: “KNOWLEDGE” OF CUSTOMER’S ILLICIT ACTIVITY

MGM GRAND & COSMOPOLITAN

DOJ

- On January 24, 2024, the former president of MGM Grand casino, Scott Sibella, pleaded guilty to failing to file suspicious activity reports when "he knew that a casino patron, Wayne Nix, ran and operated an illegal bookmaking business." DOJ stated that Sibella provided Nix complementary benefits and allowed Nix to gamble at the MGM Grand and affiliated properties with illicit funds from that bookmaking business and did not notify the casino's compliance department. According to DOJ, Sibella caused MGM Grand to fail to file a suspicious activity report. Sibella's sentencing is scheduled for May 8.
- The MGM Grand entered into a Non-Prosecution Agreement that includes a $6,527,728 fine, $500,000 forfeiture, and broad cooperation and production requirements relating to this matter for two years.
    - The casino also agreed to implement numerous enumerated enhancements to its BSA/AML Program, conduct an 18-month look-back covering MGM Grand and affiliates of SARs over $2 million that reported unknown source of funds, and submit its program enhancements and the SAR look-back to review by an External Compliance Reviewer.
- The Cosmopolitan entered into a Non-Prosecution Agreement that includes a $928,600 fine, $500,000 forfeiture, broad cooperation and production requirements relating to this matter for two years, and a general obligation to continue improving the casino's BSA/AML program.
    - The Cosmopolitan admitted in the NPA that one of its hosts knew about Nix' illegal business but allowed Nix to gamble at the casino, provided Nix with casino benefits, and didn't inform Compliance.

MindGeek

DOJ

- In December 2023, DOJ entered into a DPA with MindGeek and its affiliated regarding a novel application of the money laundering spending statute, 18 U.S.C. § 1957, for knowingly engaging in monetary transactions related to sex trafficking activity (an SUA).
- Specifically, DOJ's theory centered on MindGeek's relationship with two of its content partners, from whom MindGeek received payments to place unique channels on its websites and commissions.
- Notably, DOJ alleged that MindGeek had knowledge the funds it received were the proceeds of sex trafficking on account of:
    - Receipt of a business records subpoena from plaintiffs' counsel in a civil lawsuit filed the content partners.
    - Takedown requests by plaintiffs in the lawsuit and their counsel.
    - Criminal indictments of the content partners and their executives.
    - News alerts received and discussed by MindGeek employees.
- MindGeek agreed to pay $974,692 and enter into a three-year monitorship.
- Further, MindGeek also agreed to pay alleged victims who can demonstrate harm the full amount of their losses (excluding losses for pain and suffering), including a minimum of $3,000 per victim.

BSA/AML AND SANCTIONS

COMPLIANCE BEST PRACTICES AND REGULATORY EXPECTATIONS

04

Recent DOJ Policy Updates

In 2023, DOJ and other key U.S. law enforcement and regulatory agencies have announced a series of updates to their guidance regarding corporate enforcement and compliance, including:

New Criminal Division Corporate Enforcement & Voluntary Self-Disclosure Policy

- Issued in January 2023, the new policy updates a 2016 policy and outlines the requirements for companies to receive credit for cooperation, disclosure, and remediation in investigations.
- The new policy, now applicable to the entire Criminal Division, increases the maximum credits available to companies that cooperate, remediate, and/or voluntarily disclose, and includes additional guidance about the application of the Sentencing Guidelines in corporate resolutions.
- In February 2023, DOJ extended materially the same guidance to all 93 U.S. Attorney's Offices around the country.
- In October 2023, DOJ articulated a new safe-harbor policy for voluntary self-disclosures related to M&A transactions.

Updated Memo Regarding Evaluation of Corporate Compliance Programs

- Update to prior version, adding questions that prosecutors considering a corporate prosecution should ask regarding compensation structures that incentivize compliance and disincentivize noncompliance.
- Emphasizes communication and monitoring regarding disciplinary processes.
- Addresses risks associated with use of personal devices and different types of communication platforms, including ephemeral messaging applications.

Revised Memo Regarding Selection of Monitors in Criminal Division Matters

- Instructs prosecutors to consider the strength of a company's compliance program at the time of resolution and prior history of misconduct in making monitor decisions.

Other Recent Government Policy Updates

GIBSON DUNN

Additional notable guidance recently announced by key U.S. law enforcement and regulatory agencies includes:

DOJ Criminal Division Pilot Program Regarding Compensation Incentives and Clawbacks

- The Criminal Division (for the next three years) will include in corporate criminal resolutions provisions requiring the subject company to develop compliance-promoting criteria within its compensation and bonus systems, and the Division will offer offsetting credits to penalties for amounts clawed back from culpable employees and executives.

SEC Clawback Rule (10D-1)

- Directs national securities exchanges to issue listing standards requiring issuers to implement executive compensation clawback policies related to restatements of financial accounting.

Tri-Seal Compliance Note Regarding Sanctions and Export Controls Disclosures

- Memorandum issued by DOJ National Security Division, the Commerce Department's Bureau of Industry and Security (BIS), and Treasury Department's Office of Foreign Assets Control (OFAC) setting forth each agency's views regarding the voluntary self-disclosure of violations of U.S. sanctions and export controls laws and regulations.
- The DOJ section establishes a presumption that a company that voluntarily self-discloses will receive a non-prosecution agreement and avoid paying a fine so long as (1) the disclosure is submitted within a "reasonably prompt" time, (2) the company fully cooperates, (3) the company timely and appropriately remediates any violations, and (4) no aggravating factors (egregious/pervasive conduct, concealment, or senior management involvement) are present.
- BIS will treat deliberate nondisclosure of significant possible violations as aggravating, and give cooperation credit for disclosures of potential violations by third parties.
- OFAC reiterated that prompt disclosures can result in a 50% reduction in base penalty.

AML Compliance Programs

Compliance program best practices:

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

Risk-Based AML Program

- Under the BSA, financial institutions must maintain a risk-based, written AML Program "reasonably designed" to prevent money laundering and terrorist financing and ensure compliance with applicable BSA requirements.
  - A regularly updated risk assessment is the backbone of an AML program and should be regularly updated, including for new products, services, customer base, and geographic locations.
- Although regulators do not require the use of any particular technology or system, they encourage (and expect) use of innovative technology to increase the efficacy of BSA/AML Programs.
- It is imperative that compliance programs grow and evolve alongside growth and changes in the business.

Sanctions Compliance Best Practices

OFAC expects organizations to "employ a risk-based approach to sanctions compliance."

- In 2019, OFAC published A Framework for OFAC Compliance Commitments, identifying five essential components of a strong sanctions compliance program:

- Recent enforcement actions (including those against Tango Card, Inc. and Newmont Corporation) continue to highlight the importance of maintaining a strong sanctions compliance program, such as restricted party and geolocation screening mechanisms designed to adequately address the risks of the business.

OFAC Sanctions Compliance

Guidance for Instant Payment Systems

- In September 2022, OFAC issued guidance on Instant Payment Systems to help financial institutions minimize sanctions risk from processing transactions without the normal review process.
- This guidance stated that financial institutions should adopt a risk-based approach that begins with a risk assessment. Elevated risk factors include:
  - Engagement in cross-border payments, as opposed to only domestic payments;
  - Transactions involving foreign banks or foreign persons with whom the customer has not previously dealt; and
  - Transaction amounts inconsistent with customer's prior history.
- Financial institutions can further decrease risk by:
  - Incorporating sanctions compliance during the design and development process of the instant payment systems;
  - Establishing minimum sanctions compliance expectations for co-parties, such as customer onboarding and ongoing due diligence standards; and
  - Using or developing AI and automated systems that (i) automatically communicate information between participating institutions and (ii) allow the system to pause suspect transactions for further review (e.g., exception processing).

Other AML Compliance Program Considerations

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

EXPECTATIONS FOR 2024 AND BEYOND

05

AML Landscape in 2024 and Beyond

1

Continued implementation of AML Act of 2020

2

Expansions of BSA coverage

Residential and Commercial Real Estate, Investment Advisors, and potentially art and antiquities dealers and third-party payment service providers.

3

Continued increasing regulator scrutiny and enforcement related to digital assets

between the enforcement priority placed on virtual currency activities and greater AML whistleblower incentives and protections.

4

Increased focus on payments and fintech relationships

Likely OFAC Priorities in the Year Ahead

- **Russia:**
  Continued all-of-government approach to exert pressure on Russia in light of the war in Ukraine. This will likely include additional designations to the SDN List, continued compliance guidance, and possible adjustment of the oil and petroleum products price caps, additional seizure of properties belonging to restricted parties, and potential additional export restrictions.
- **Venezuela:**
  Ground-breaking new general licenses issued in October 2023, significantly ease sanctions on Venezuela's energy and mining sectors, and permit secondary trading in certain Venezuelan government debt and equity. Duration of these measures will depend upon implementation of agreed-upon electoral reforms between the Maduro regime and opposition leaders.
- **Iran:**
  Sustained pressure in light of Iran's support for Russia's military operations, continued ballistic missile procurement activities, and apparent support for Hamas militants in Gaza.
- **China:**
  Continued all-of-government approach to address the "pacing challenge" of China's economic rise and increasing attempts to curb Chinese access to new and emerging technologies, as well as potential bans on U.S. outbound investments.
- **Cryptocurrency Payments & Novel Technologies:**
  Continued assessment by OFAC of unique compliance concerns posed by cryptocurrency payments and other novel technologies.
- **Multilateral Efforts:**
  Continued reliance on multilateral efforts for sanctions enforcement (and export controls), particularly with respect to China and Russia. Such efforts are likely to continue in the coming months.

ATTORNEY BIOS

1050 Connecticut Avenue, N.W., Washington, DC 20036-5306 USA
T +1 202.887.3609
fwarin@gibsondunn.com

F. Joseph Warin

Partner / Washington, D.C.

F. Joseph Warin is chair of the 250-person Litigation Department of Gibson Dunn's Washington, D.C. office, and he is co-chair of the firm's global White Collar Defense and Investigations Practice Group. 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 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 practice also 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.

Mr. Warin's full biography can be viewed here.

EDUCATION

Georgetown University
Juris Doctor

Creighton University
Bachelor of Arts

SELECTED RECOGNITIONS
Securities: Regulation: Enforcement, FCPA, Litigation: White-Collar Crime & Government Investigations, Litigation: Securities
- 2023 Chambers USA

EDUCATION

Georgetown University
Juris Doctor

Northwestern University
Bachelor of Science

SELECTED RECOGNITIONS
White Collar Trailblazer, a Global Investigations Review Top 100 Women in Investigations

NLJ Awards Finalist for Professional Excellence – Crisis Management & Government Oversight
- National Law Journal

1050 Connecticut Avenue, N.W., Washington, DC 20036-5306 USA
T +1 202.887.3502
sbrooker@gibsondunn.com

Stephanie Brooker

Partner / Washington, D.C.

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'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); digital assets and fintech; securities, tax, and wire fraud, foreign influence; work place misconduct/"me-too"; 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's full biography can be viewed here.

EDUCATION

Harvard University
Juris Doctor

University of Oxford
Master of Philosophy

Brown University
Bachelor of Arts

SELECTED RECOGNITIONS
International Trade: Export Controls and Economic Sanctions
- 2023 Chambers USA

Thought Leader: Trade & Customs - International Sanctions
- Who's Who Legal

1050 Connecticut Avenue, N.W., Washington, DC 20036-5306 USA
T +1 202.887.3547
asmith@gibsondunn.com

Adam M. Smith

Partner / Washington, D.C.

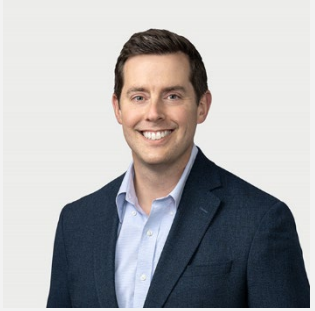
Adam M. Smith is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher and serves as co-chair of the firm's International Trade Practice Group. He is an experienced international lawyer with a focus on international trade compliance and white collar investigations, including with respect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

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 in the White House. 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 traveled 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.

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.

Mr. Smith's full biography can be viewed here.



EDUCATION

University of Virginia
Juris Doctor

University of Kansas
Bachelor of Arts

SELECTED RECOGNITIONS
Litigation: White-Collar Crime & Government Investigations
- 2023 Chambers USA

White-Collar and Criminal Defense
- 2024 Best Lawyers in America

1050 Connecticut Avenue, N.W., Washington, DC 20036-5306 USA
T +1 202.955.8220
kday@gibsondunn.com

M. Kendall Day

Partner / Washington, D.C.

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

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

Prior to joining Gibson Dunn, Mr. Day had a distinguished 15-year career as a white collar prosecutor with the Department of Justice (DOJ), rising to the highest career position in the DOJ's Criminal Division as an Acting Deputy Assistant Attorney General (DAAG). As a DAAG, 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. 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's full biography can be viewed here.

EDUCATION

New York University
Juris Doctor

Fordham University
Bachelor of Science

OTHER QUALIFICATIONS
CAMS Certified

SELECTED RECOGNITIONS
Fintech: Rising Star
- 2023 Law 360

White Collar Litigation and Investigations
- 2023 Lawdragon 500 X – The Next Generation

White Collar: Rising Star
- 2023 – 2022 Super Lawyers

1050 Connecticut Avenue, N.W., Washington, DC 20036-5306 USA
T +1 202.887.3511
ecapone@gibsondunn.com

Ella Alves Capone

Of Counsel / Washington, D.C.

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

Ms. Capone's practice focuses on advising multinational corporations and financial institutions on Bank Secrecy Act/anti-money laundering (BSA/AML), anti-corruption, sanctions, and consumer financial regulatory and enforcement matters, with a particular focus on advising banks, gaming businesses, payment entities, online marketplaces, cryptocurrency businesses and other fintech entities. She regularly advises clients on the implementation, enhancement, and assessment of their compliance programs and internal controls, platform terms and conditions, and product and business strategies for regulatory compliance of innovative financial solutions. Ms. Capone is CAMS certified and frequently provides clients with training on financial services regulations and corporate compliance programs, including enforcement trends, industry best practices, and regulator expectations.

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

Ms. Capone's full biography can be viewed here.

EDUCATION

Stanford University
Juris Doctor

University of Southern California
Bachelor of Arts

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

333 South Grand Avenue, Los Angeles, CA 90071-3197

T + 1 213.229.7786

crjones@gibsondunn.com

Chris R. Jones

Senior Associate / Los Angeles

Chris Jones is a senior associate in the Los Angeles office of Gibson, Dunn & Crutcher. He is a member of the White Collar Defense and Investigations, Litigation, Anti-Money Laundering, and National Security groups. His practice focuses primarily on internal investigations and enforcement defense, regulatory and compliance counseling, and complex civil litigation.

Previously, Mr. Jones clerked for the Honorable Timothy J. Kelly of the United States District Court for the District of Columbia. He also practiced in the litigation department of a major international law firm for three years.

Mr. Jones received his J.D. from Stanford Law School in 2014. While in law school, he served as an Articles Editor for the *Stanford Law Review* and the Co-Executive Director of the Afghanistan Legal Education Project. Mr. Jones is a member of the American Bar Association and the Los Angeles County Bar Association.

Mr. Jones' full biography can be viewed here.

GIBSON DUNN