AVILA

Avila Rodriguez Hernandez Mena & Garro LLP

2025 Navigating OFAC's Evolving Landscape

Patricia M. Hernandez

BSA/AML Symposium

October 27, 2025

FLORIDA BANKERS ASSOCIATION

TODAY'S OBJECTIVES

- Discussion on new recordkeeping requirements.
- Address certain compliance **trends and changes** related to:
  - Russia
  - Cyber Sanctions and Ransomware
  - Global Magnitsky Sanctions
  - Venezuela and Cuba
- Recent Enforcement Actions

OFAC SANCTIONS PROGRAMS:

- Afghanistan-Related Sanctions
- Balkans-Related Sanctions
- Belarus Sanctions
- Burma (Myanmar)-Related Sanctions
- Central African Republic Sanctions
- China / Chinese Military Companies Sanctions
- Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA)
- Counter Narcotics Trafficking Sanctions
- Counter Terrorism Sanctions
- **Cuba Sanctions**
- **Cyber-Related Sanctions**
- Democratic Republic of the Congo-related Sanctions
- Ethiopia-Related Sanctions
- Foreign Interference in a United States Election Sanctions
- **Global Magnitsky Sanctions**
- Hong Kong-Related Sanctions
- Hostages and Wrongfully Detained U.S. Nationals Sanctions
- Iran Sanctions
- Iraq-Related Sanctions
- Lebanon-Related Sanctions
- Libya Sanctions
- Mali-Related Sanctions
- Nicaragua-Related Sanctions
- Non-Proliferation Sanctions
- North Korea Sanctions
- Rough Diamond Trade Controls
- Somalia Sanctions
- Sudan and Darfur Sanctions
- South Sudan-Related Sanctions
- Syria Sanctions (inactive as of July 1, 2025)
- Transnational Criminal Organizations
- **Ukraine-/Russia-Related Sanctions**
- **Venezuela-Related Sanctions**
- Yemen-Related Sanctions
- Zimbabwe Sanctions

OFAC FRAMEWORK FOR COMPLIANCE

OFAC COMPLIANCE FRAMEWORK

- On May 2, 2019, OFAC published a "**Framework for OFAC Compliance Commitments**" to provide organizations subject to U.S. jurisdiction with OFAC's perspective on the essential components of a sanctions compliance program ("SCP").
  - *"As the U.S. continues to enhance our sanctions programs, ensuring that the private sector implements strong and effective compliance programs that protect the U.S. financial system from abuse is a key part of our strategy."*
- OFAC noted some of the **root causes of apparent violations** of U.S. economic and trade sanctions programs, including:
  - **Lack of formal OFAC Sanctions Compliance Program**
  - Issues with **screening software updates and filters**
  - **Improper due diligence** on customers and clients
  - **De-centralized compliance functions** and inconsistent application of a sanctions compliance program
  - **Misinterpreting or failing to understand** OFAC sanctions

OFAC COMPLIANCE FRAMEWORK

Five Essential Components:

- Management Commitment
- Risk Assessment
- Internal Controls
- Testing and Auditing
- Training

NEW RECORDKEEPING REQUIREMENTS

- On April 24, 2024, President Biden signed into law the “21st Century Peace Through Strength Act,” which extended the statute of limitations for civil and criminal violations of sanctions from five years to ten years.
- OFAC adopted a final rule (effective March 21, 2025) extending its required record retention period from 5 years to 10 years for records subject to OFAC’s jurisdiction.
  - This amendment is to 31 C.F.R. § 501.601: persons engaging in any transaction subject to U.S. sanctions regulations shall **keep a full and accurate record of each such transaction engaged in**, regardless of whether such transaction is licensed or unlicensed, and such record shall be available for examination for at least 10 years after the date of such transaction.
- The rules apply prospectively (to transactions going forward), but because the statute of limitations extension is retroactive in part (for actions not yet time-barred), organizations may need records going back to April 2019 for violations not yet time-barred.
- **Financial institutions must reassess their record retention policies and update internal frameworks to comply with the new 10-year requirement. Regulatory agencies will expect institutions to revise policies, procedures, and controls to reflect this change. Systems will need to accommodate additional storage, indexing, and retrieval over longer periods.**

OFAC SANCTIONS: RUSSIA

DIRECTIVE 1A UNDER EXECUTIVE ORDER 14024

- "Prohibitions Related to Certain Sovereign Debt of the Russian Federation"
  - Expands the existing sovereign debt restrictions imposed by Directive 1 under E.O. 14024, which only applied to the primary market and lending restrictions
  - Prohibits U.S. financial institutions from participating in the primary market issued by the Central Bank of Russia, the National Wealth Fund of Russia, or the Ministry of Finance of Russia after June 14, 2021, and secondary market for bonds issued by the same after March 1, 2022

DIRECTIVE 2 UNDER EXECUTIVE ORDER 14024

- "Prohibitions Related to Correspondent or Payable-Through Accounts and Processing of Transactions Involving Certain Foreign Financial Institutions"
  - Effective March 26, 2022
- Targets Russia's largest institution, Sberbank, and Sberbank foreign financial institution subsidiaries
- Prohibits U.S. financial institutions from opening or maintaining correspondent bank accounts or processing transactions involving sanctioned Russian banks including Sberbank

DIRECTIVE 2: ENTITIES TARGETED

- PUBLIC JOINT STOCK COMPANY SBERBANK OF RUSSIA
  - ARIMERO HOLDING LIMITED
  - IKS JOINT STOCK COMPANY
  - INSURANCE COMPANY SBERBANK INSURANCE LIMITED LIABILITY COMPANY
  - INSURANCE COMPANY SBERBANK LIFE INSURANCE LIMITED LIABILITY COMPANY
  - JOINT STOCK COMPANY RASCHETNIYE RESHENIYA
  - JOINT STOCK COMPANY SBERBANK
  - JOINT STOCK COMPANY SBERBANK AUTOMATED TRADE SYSTEM
  - JOINT STOCK COMPANY SBERBANK LEASING
  - JOINT STOCK COMPANY SBERBANK PRIVATE PENSION FUND
  - LIMITED LIABILITY COMPANY MARKET FUND ADMINISTRATION
  - LIMITED LIABILITY COMPANY PROMISING INVESTMENTS
  - LIMITED LIABILITY COMPANY SBERBANK CAPITAL
  - LIMITED LIABILITY COMPANY SBERBANK CIB HOLDING
  - LIMITED LIABILITY COMPANY SBERBANK FACTORING
  - LIMITED LIABILITY COMPANY SBERBANK FINANCIAL COMPANY
  - LIMITED LIABILITY COMPANY SBERBANK INSURANCE BROKER
  - LIMITED LIABILITY COMPANY SBERBANK INVESTMENTS
  - LIMITED LIABILITY COMPANY YOOMONEY
  - OPEN JOINT STOCK COMPANY BPS-SBERBANK
  - SB SECURITIES SA
  - SBERBANK EUROPE AG
  - SETELEM BANK LIMITED LIABILITY COMPANY
  - TEKHNOLOGII KREDITOVANIYA LIMITED LIABILITY COMPANY
  - VYDAYUSHCHIESYA KREDITY MICROCREDIT COMPANY LIMITED LIABILITY COMPANY

DIRECTIVE 3 UNDER EXECUTIVE ORDER 14024

- “Prohibitions Related to New Debt and Equity of Certain Russia-related Entities”
  - Effective March 26, 2022
- Prohibited transactions and dealings by U.S. persons or within the U.S. in new debt or new equity with:
  - Russian state-owned enterprises
  - Entities that operate in the financial services sector of the Russian Federation economy
  - Other entities determined to be subject to the prohibitions in this directive

DIRECTIVE 3: ENTITIES TARGETED

- CREDIT BANK OF MOSCOW PUBLIC JOINT STOCK COMPANY
- GAZPROMBANK JOINT STOCK COMPANY
- JOINT STOCK COMPANY ALFA-BANK
- JOINT STOCK COMPANY RUSSIAN AGRICULTURAL BANK
- JOINT STOCK COMPANY SOVCOMFLOT
- OPEN JOINT STOCK COMPANY RUSSIAN RAILWAYS
- PUBLIC JOINT STOCK COMPANY ALROSA
- PUBLIC JOINT STOCK COMPANY GAZPROM
- PUBLIC JOINT STOCK COMPANY GAZPROM NEFT
- PUBLIC JOINT STOCK COMPANY ROSTELECOM
- PUBLIC JOINT STOCK COMPANY RUSHYDRO
- PUBLIC JOINT STOCK COMPANY SBERBANK OF RUSSIA
- PUBLIC JOINT STOCK COMPANY TRANSNEFT

DIRECTIVE 4 UNDER EXECUTIVE ORDER 14024

- “Prohibitions Related to Transactions Involving the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, and the Ministry of Finance of the Russian Federation”
  - Effective February 28, 2022
- Prohibits US Persons from engaging in any transaction involving:
  - The Central Bank of the Russian Federation
  - The National Wealth Fund of the Russian Federation
  - The Ministry of Finance of the Russian Federation

DETERMINATION PURSUANT TO SECTION 1(a)(i) of EXECUTIVE ORDER 14024

- Section 1(a)(i) imposes economic sanctions on any person determined to operate or have operated in such sectors of the Russian Federation economy
- March 31, 2022 determination extends the economic sanctions to aerospace, electronics, and marine sectors of the Russian Federation economy
- May 8, 2022 determination extends the economic sanctions to accounting, trust and corporate formation services, and management consulting sectors of the Russian Federation economy

EXECUTIVE ORDER 14065

- “Blocking Property of Certain Persons and Prohibiting Certain Transactions With Respect to Continued Russian Efforts To Undermine the Sovereignty and Territorial Integrity of Ukraine”
- Imposes sanctions on the Donetsk People’s Republic (“DNR”) and Luhansk People’s Republic (“LNR”) regions of Ukraine
  - Imposed in response to the Russian Government’s decision to recognize the DNR and LNR as independent from Ukraine
- Prohibits US Persons from:
  - Engaging in new investments in the Covered Regions
  - Importing into the United States any goods, services, or technology from the Covered Regions
  - Exporting, reexporting, selling, or suppling, directly or indirectly, any goods, services, or technology to the Covered Regions
  - Providing any approval, financing, facilitation, or guarantee of a transaction by a non-US party where the transaction would be prohibited if performed by a US Person with respect to the Covered Regions

EXECUTIVE ORDER 14066

- “Prohibiting Certain Imports and New Investments With Respect to Continued Russian Federation Efforts to Undermine the Sovereignty and Territorial Integrity of Ukraine”
- Prohibits:
  - Import of Russian oil, liquefied natural gas, and coal to the United States
  - New investment in the energy sector in the Russian Federation by a United States person
  - Any approval, financing, facilitation, or guarantee by a United States person of a transaction by a foreign person where the transaction by that foreign person would be prohibited by this section if performed by a United States person or within the United States

EXECUTIVE ORDER 14068

- “Prohibiting Certain Imports, Exports, and New Investment with Respect to Continued Russian Federation Aggression”
- Prohibits the importation into the U.S. of the following products of Russian Federation origin:
  - Fish, seafood, and preparations thereof
  - Alcoholic beverages
  - Non-industrial diamonds
- Bans the exportation, re-exportation, sale, or supply, directly or indirectly, from the U.S. or by a U.S. person, of:
  - Luxury goods
  - U.S. dollar-denominated banknotes to the Government of Russia or to any person located in the Russian Federation

DETERMINATION PURSUANT TO SECTION 1(a)(i) OF EXECUTIVE ORDER 14068

- Prohibitions will apply to gold of Russian Federation origin
  - Importation into U.S. of gold is prohibited
  - Excludes gold of Russian Federation origin that was located outside of the Russian Federation prior to the effective date of this determination

EXECUTIVE ORDER 14071

- “Prohibiting New Investment in and Certain Services to the Russian Federation in Response to Continued Russian Federation Aggression”
- Prohibits
  - New investment in the Russian Federation by a U.S. person
  - Exportation, re-exportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any category of services as may be determined by the Secretary of the Treasury, in consultation with the Secretary of State, to any person located in the Russian Federation
  - Any approval, financing, facilitation, or guarantee by a United States person, wherever located, of a transaction by a foreign person where the transaction by that foreign person would be prohibited by this section if performed by a United States person or within the United States.

DETERMINATION PURSUANT TO SECTION 1(a)(i) OF EXECUTIVE ORDER 14071

- Effective June 7, 2022
- Prohibitions will apply to the following categories of service: accounting, trust and corporate formation, and management consulting
- Prohibited activities include the exportation, re-exportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of accounting, trust and corporate formation, or management consulting services to any person located in the Russian Federation.
- This determination excludes:
  - Any service to an entity located in the Russian Federation that is owned or controlled, directly or indirectly, by a United States person
  - Any service in connection with the wind down or divestiture of an entity located in the Russian Federation that is not owned or controlled, directly or indirectly, by a Russian person

OFAC SANCTIONS: CYBER SANCTIONS

CYBER-RELATED SANCTIONS

- Began on **April 1, 2015**.
- President Obama issued **E.O. 13694** and declared a **national emergency** to deal with the unusual and extraordinary threat to the **national security, foreign policy, and economy** of the U.S. by the increase of malicious cyber-enabled activities originating from, or directed **by persons located outside the U.S.**
  - **E.O. 13694** authorizes the imposition of sanctions against persons responsible for or complicit in, or to have engaged in, certain malicious cyber-enabled activities.
- On **December 28, 2016,** President Obama issued **E.O. 13757**, which amended E.O. 13694 by adding an **Annex and authorizing sanctions** related to:
  - Tampering with or misappropriating information with the purpose or effect of interfering with election processes or institutions, and
  - Activities intended to undermine democratic institutions or influence political outcomes.

CYBER-RELATED SANCTIONS: E.O. 13694

- **E.O. 13694** is intended to address situations where, for jurisdictional or other issues, certain significant malicious cyber actions may be beyond the reach of other authorities available to the U.S. government. Allows OFAC to place such persons on the SDN List.
- As a general matter, **U.S. persons, including firms that facilitate or engage in online commerce,** are responsible for ensuring they do not engage in unauthorized transactions or dealings with persons on SND List or operate in jurisdictions targeted by sanctions programs.
- For purposes of **E.O. 13694, malicious cyber-enabled activities include:**
  - **Deliberate activities** accomplished through unauthorized access to a computer system, including by remote access;
  - **Circumventing** one or more protection measures, including by bypassing a firewall; or
  - **Compromising** the security of hardware or software in the supply chain.
- These activities are often the **means through which the specific harms** enumerated in the E.O. are achieved, including:
  - **Compromise** to critical infrastructure,
  - **Denial** of service attacks, or
  - **Massive loss of sensitive information**, such as trade secrets and personal financial information.

OFAC ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS

- On **October 1, 2020**, OFAC issued an Advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities.
  - The Advisory warns against **U.S. persons making and those that facilitate making ransomware payments** to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response.
  - OFAC warns that these payments not only encourage future ransomware payment demands, but also may risk violating OFAC cyber-related regulations.
- The Advisory was amended and superseded on **September 21, 2021**.
  - Sharpens guidance on expectations, emphasizes greater discouragement of ransom payments, and supplies more detail on mitigating factors it would consider in enforcement.
  - Emphasizes that cooperation with law enforcement is key.

FACILITATING RANSOMWARE PAYMENTS ON BEHALF OF A VICTIM MAY VIOLATE OFAC REGULATIONS

- The Advisory warns of making ransomware payments directly, but also through intermediaries.
- OFAC believes such payments benefit illicit actors and can undermine the national security and foreign policy objectives of the U.S.
- Therefore, license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial.
- It warns that U.S. persons, wherever located, are generally prohibited from **facilitating** actions, which could not be directly performed by U.S. persons due to U.S. sanctions regulations.
    - Enforcement focus has shifted from principal attackers to enablers in recent years.
- These may include providers of cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments.

AMENDMENT TO THE CYBER-RELATED SANCTIONS REGULATIONS

- OFAC has **amended, and reissued in their entirety, the Cyber-Related Sanctions Regulations**, 31 C.F.R. part 578, effective as of September 6, 2022 through its publication in the Federal Register.
  - Further implements both **E.O. 13694 (**April 1, 2015), as then amended by **E.O. 13757 (**December 28, 2016) issued by President Obama.
  - Also includes certain provisions of the Countering America's Adversaries Through Sanctions Act.

RECENT EXECUTIVE ORDERS

- On January 16, 2025, President Biden issued **E.O. 14144**, which further amended prior cyber-sanctions authorities to broaden Treasury's tools for cyber-related hostile acts and lower the threshold at which OFAC is authorized to bring actions.
- On June 6, 2025, President Trump issued **E.O. 14306**, which amends provisions of **E.O. 14144** related to software supply chain security, artificial intelligence, quantum computing, and key federal guidance documents.

CYBER-RELATED SANCTIONS TODAY

- OFAC continues to treat cyber-enabled malicious activity as a priority subject for sanctions.
  - Central focus on targeting facilitators/enablers: virtual-currency mixers, exchanges, OTC traders, and financial service providers that enable laundering of ransomware/other cyber proceeds and monetize stolen funds
  - Expansion of targeting to fintech operators & tokenization platforms
- Sanctions have been paired with indictments, asset seizures, FinCEN advisories, and foreign partner engagement to disrupt networks end-to-end.

OFAC SANCTIONS: GLOBAL MAGNITISKY

SERGEI MAGNITSKY RULE OF LAW ACCOUNTABILITY ACT OF 2012

- The Sergei Magnitsky Rule of Law Accountability Act originated in 2012.
- The Magnitsky Act authorized sanctions upon persons responsible (or their accomplices), or those who participated in, the death of Sergei Magnitsky or committed other human rights violations in the Russian Federation.

GLOBAL MAGNITSKY HUMAN RIGHTS ACCOUNTABILITY ACT (2016)

- In 2016, Congress passed the Global Magnitsky Human Rights Accountability Act, which globalized the effects of the 2012 law.
- Allows the revocation of U.S. entry visas.
- Allows the blocking of persons who:
  - Are responsible for the killing, torture or other human rights violations against persons who work to expose illicit activities of a government or those who work to protect human rights, including rights to free elections; or
  - Are officials of a corrupt government, or persons related to such officials or who facilitate such activities, including expropriation of private property or money laundering.

EXECUTIVE ORDER 13818 (2017)

- The Global Magnitsky Human Rights Accountability Act was implemented through Executive Order 13818 (December 2017).
  - Gives the Executive branch authority to block property and impose sanctions on foreign persons involved in serious human rights abuse or corruption globally.

DESIGNATIONS

- In 2024, the United States designated 70 foreign persons under the Global Magnitsky sanctions program, bringing the total foreign persons designated under the program to over 740.
  - Represents the most geographically expansive set of designations to date, including targets in over 19 countries from nearly every major geographic region.

OFAC SANCTIONS: VENEZUELA

VENEZUELA SANCTIONS: PROHIBITED TRANSACTIONS

- The U.S. has employed sanctions as a **policy tool** in response to activities of the Venezuelan government or Venezuelan individuals, including:
  - U.S. first imposed sanctions in 2015.
  - **The Government of Venezuela remains blocked.**
- Since the Trump administration's return in 2025, there has been a "snap back" in stricter sanctions posture. Some relief previously granted has been (or is likely to be) reversed.

OFAC SANCTIONS: CUBA

CUBA SANCTIONS: BACKGROUND

- The **Cuban Assets Control Regulations** (“CACR”) were issued by the U.S. Government on July 8, 1963, under the Trading with the Enemy Act (“TWEA”) in response to certain hostile actions by the Cuban Government.
- The CACR was amended by OFAC and published in the Federal Register on June 9, 2022 to further implement portions of the President’s foreign policy toward Cuba.
- In 2025, OFAC reached a settlement with Key Holding, LLC for violations related to Cuban transactions involving a subsidiary.
- Biden administration changes include:
  - Family reunification
  - Authorized travel
  - U.S. internet
  - Increase remittances

CUBA SANCTIONS

- CACR applies to **all persons** (individuals and entities) **subject to U.S. jurisdiction**, including:
  - All U.S. citizens and permanent residents **wherever located**,
  - All persons **in the U.S**.,
  - All **branches and subsidiaries** of U.S. organizations **throughout the world**, and
  - **All persons** engaging in transactions that **involve property in or otherwise** subject to the **jurisdiction of the U.S.**

ENFORCEMENT ACTIONS

IMPORTANT ENFORCEMENT ACTIONS

- Between January 2025 to September 2025
  - 9 public enforcement actions.
  - Year-to-date totals for penalties and settlements: $238,249,250.
- Older relevant cases:
  - TD Bank
  - Emigrant Bank
  - MidFirst Bank
  - Banco Popular Puerto Rico

OFAC VIOLATIONS: ShapeShift AG

- **September 2025**
- OFAC announced a **$750,000 settlement** with ShapeShift AG, a digital asset exchange incorporated in Switzerland and operating from Denver, Colorado.
- Violations occurred when ShapeShift engaged in digital asset transactions on its exchange platform with users located in Cuba, Iran, Sudan, and Syria.
- OFAC determined that the violations were **non-egregious** and **not voluntarily self-disclosed**.
- This enforcement action highlights the importance for digital asset actors subject to U.S. jurisdiction of implementing effective, risk-based sanctions compliance controls.

OFAC VIOLATIONS: Fracht FWO Inc.

- **September 2025**
- OFAC announced a **$1,610,775 settlement** with Fracht FWO Inc., an international freight forwarder with its principal place of business in Houston, Texas.
- Violations occurred when Fracht, by failing to follow internal compliance procedures, contracted with a blocked Government of Venezuela airline to transport goods from Mexico to a customer in Argentina.
  - To fulfill the contract, the blocked Venezuelan airline used an aircraft separately blocked by OFAC for being operated by Iran's Mahan Air and crewed by Iranian nationals—conduct reflecting apparent violations of OFAC's Iran, proliferation, and terrorism sanctions programs.
- OFAC determined that the violations were **egregious** and **not voluntarily self-disclosed**.
- This enforcement action emphasizes the importance for international trade service providers, such as freight forwarders, to know their counterparties and recognize the risks of prioritizing urgent business demands at the expense of compliance.

OFAC VIOLATIONS: Interactive Brokers LLC

- **July 2025**
- OFAC announced a **$11,832,136 settlement** with Interactive Brokers LLC (“IB”), a Greenwich, Connecticut-based global electronic broker-dealer providing brokerage and investment services to millions of customers worldwide through its online brokerage platform.
- Violations occurred when IB provided brokerage and investment services to persons in Iran, Cuba, Syria, and the Crimea region of Ukraine (“Crimea”), processed trades in securities subject to the Chinese Military-Industrial Complex program, conducted transactions involving blocked persons under OFAC’s Russia, Global Magnitsky, Venezuela, and Syria sanctions programs, and engaged in new investment in the Russian Federation.
- OFAC determined that the violations were **non-egregious** and **voluntarily self-disclosed**.
- This enforcement action underscores the importance of obtaining and using all available information to verify a customer’s location or ordinary residency; the importance of accurately assessing the sanctions risk presented by particular service offerings, and the need for appropriate investment in sanctions compliance headcount.

OFAC VIOLATIONS: Harman International Industries, Inc.

- **July 2025**
- OFAC announced a **$1,454,145 settlement** with Harman International Industries, Inc., a Connecticut-based multinational audio electronics company.
- Violations occurred when overseas employees of a U.S. subsidiary of Harman enabled the diversion of its products from its United Arab Emirates (UAE) distributor to Iran.
- OFAC determined that the violations were **egregious** and **voluntarily self-disclosed**.
- This enforcement action demonstrates the risks that foreign employees of U.S. companies can create for their employers in the absence of controls sufficient to prevent noncompliance.

OFAC VIOLATIONS: Key Holding, LLC

- **July 2025**
- OFAC announced a **$608,825 settlement** with Key Holding, LLC, a privately held global logistics company based in Delaware.
- Violations occurred when Key Holding, LLC's Colombian subsidiary managed the logistics for 36 freight shipments from Colombia to Cuba.
- OFAC determined that the violations were **not-egregious** and **voluntarily self-disclosed**.
- This enforcement action highlights the importance of ensuring that newly acquired subsidiaries, including entities organized outside the United States, are aware of and comply with their obligations under the CACR, which extends to entities owned or controlled by U.S. persons, such as foreign subsidiaries.

OFAC VIOLATIONS: Unicat Catalyst Technologies, LLC

- **June 2025**
- OFAC announced a **$3,882,797 settlement** with Unicat Catalyst Technologies, LLC, Texas-based company that sells and consults on catalyst products used in petrochemical refinery and steel mill operations, as successor to Unicat Catalyst Technologies, Inc., and its subsidiaries, assignees, successors, and affiliates worldwide.
- Violations occurred when Unicat's former chief executive officer and co-founder and former employees and representatives supplied catalyst products and consulting services to customers in Iran and sold goods to a blocked Venezuelan entity.
- OFAC determined that the violations were **egregious** and **voluntarily self-disclosed**.
- This enforcement action demonstrates the risks involved in dealing with sanctioned jurisdictions and persons, and underscores the importance of institutionalizing a culture of compliance that can prevent employees and management from successfully directing violations of U.S. sanctions.

OFAC VIOLATIONS: GVA Capital, Ltd.

- **June 2025**
- OFAC announced a **$215,988,868 settlement** with GVA Capital, Ltd., a venture capital firm based in San Francisco, California.
- Violations occurred when GVA Capital knowingly managed an investment for sanctioned Russian oligarch Suleiman Kerimov while aware of his blocked status.
- OFAC determined that the violations were **egregious** and **not voluntarily self-disclosed**.
- This enforcement action underscores the importance of gatekeepers in preventing sanctions evasion and highlights the risks of facilitating such efforts.

OFAC VIOLATIONS: Haas Automation, Inc.

- **January 2025**
- OFAC announced a **$1,044,781 settlement** with Haas Automation, Inc., a manufacturer of machine tools and related parts based in California.
- Violations occurred when Haas indirectly supplied one computer numerical control (CNC) machine, 13 orders of spare parts, and seven authorization codes for CNC machines owned by blocked Russian entities.
- OFAC determined that the violations were **not voluntarily self-disclosed** and 8 out of 21 apparent violations were **egregious**.
- This enforcement action highlights the importance of considering risks posed by customers with which companies maintain an ongoing relationship, including through the provision of after-sale services, such as through the selling of spare parts or other goods and services to sustain a product's continued operation.

OFAC VIOLATIONS: Family International Realty LLC

- **January 2025**
- OFAC announced a **$1,076,923 settlement** with Family International Realty LLC, a Miami, Florida-based real estate company, and a US Person.
- Violations occurred when the U.S. Person and the Company engaged in a willful scheme to evade OFAC sanctions by transferring nominal ownership of three luxury condominiums owned by two sanctioned Russian oligarchs, Valeri Abramov and Viktor Perevalov, to their non-sanctioned family members and to shell companies owned by those family members.
- OFAC determined that the violations were **egregious** and **not voluntarily self-disclosed**.
- This enforcement action highlights the role that gatekeepers—including realtors, investment advisers, attorneys, and trust and corporate services providers—can play in enabling sanctions evasion.

RELEVANT ENFORCEMENT TOPICS

- Use of U.S. financial system, regardless of currency.
- Non-standard payment.
- Export or re-export of U.S. origin goods.
- U.S. parent liability for non-U.S. subsidiary business.
- Deficient Due Diligence.
- Failing to understand sanctions.
- Screening software limitations.
- Mergers and Acquisitions.
- Individual Liability.

OFAC COMPLIANCE PROGRAMS: UNDETECTED VIOLATIONS

- **Potential violations** should be reported to a designated internal contact and **counsel should be advised.**
- If the violation is ongoing, all activity regarding the transaction or relationship should **cease immediately.**
- An **internal investigation** should be conducted and if necessary, outside counsel should be engaged.
- To the extent a violation is confirmed, a **self-disclosure** should be filed with OFAC.
- **Review OFAC compliance program policies and procedures** to determine what went wrong and determine what improvements need to be made.
- Conduct a **look-back** for similar cases and **implement improved policies and procedures** based on the investigations.

TRENDS AND PATTERNS

- Egregious vs. Non-Egregious Violations: OFAC draws a strong line between serious/egregious violations (involving concealment, knowledge by senior management, use of intermediaries, deliberate evasion) and those less so. Penalties are much higher when egregiousness is present.
- Self-Disclosure Matters: Voluntary self-disclosure and cooperation tend to reduce penalties significantly.
- Multiple Sanctions Programs: Many cases involve violations under more than one sanctions regime (e.g. Iran, Russia / Ukraine, Cuba, Global Magnitsky). Aggregate conduct increases exposure.
- Intermediaries & Foreign Affiliates: Entities are trying to use non-U.S. subsidiaries or foreign affiliates, third parties, to route around or obscure sanctions exposure. OFAC is aggressive in looking through such structures.
- Crypto / Digital Assets: Cases like ShapeShift show that digital asset platforms are on OFAC's radar, especially transactions involving persons in sanctioned jurisdictions.
- Post-Acquisition Awareness: As in Key Holding's case, when a U.S. company acquires foreign subsidiaries, those subsidiaries may become subject to U.S. sanctions laws.

OTHER UPDATES

- Conflicts of law (for example, EU requirements that certain financial records be deleted after 5 years) do not excuse noncompliance with the OFAC 10-year recordkeeping requirement. However, OFAC may consider such conflicts as mitigating factors in enforcement.
  - Banks with international footprint must carefully reconcile and document their retention policies.
- Many OFAC reports (initial reports of blocked property, rejected transaction reports, and the Annual Report of Blocked Property) generally must be submitted via the OFAC Reporting System (ORS), rather than by email or mail.
- U.S. persons must report any unblocking or transfer of property that had been blocked, within 10 business days of the event, unless specific exceptions apply.
- When OFAC believes an account or transaction “may involve” property of a blocked person, it may issue instructions to financial institutions to provide information about such transactions, even if not originally blocked.
  - Banks should be prepared to respond to OFAC requests for transactional details, internal logs, and screening histories, even for transactions not initially flagged or blocked.
- OFAC may impose late-filing penalties for required reports for 10 years.

CASE STUDY

- Customer Export Transaction.
- Employee Error.
- Lack of Training.
- Self Disclosure.

Q&A

PRESENTER

Patricia M. Hernandez
Founding Partner

Avila Rodriguez Hernandez Mena & Garro LLP
2525 Ponce de Leon Blvd, Penthouse 12th Floor
Coral Gables, FL 33134
Tel: 305.779.3566
Fax: 305.779.3561
phernandez@avilalaw.com