Strafford
A BARBRI Company

Presenting a live 90-minute webinar with interactive Q&A

OFAC Compliance: Meeting Evolving U.S. Sanctions Requirements, Minimizing Risk of Sanctions

WEDNESDAY, AUGUST 13, 2025

1pm Eastern 12pm Central 11am Mountain 10am Pacific

- Peter E. Jeydel, Partner, Sanctions & Trade Controls Group Leader, **Troutman Pepper Locke**, Washington, D.C.
- Will Schisa, Counsel, **Davis Polk & Wardwell**, Washington, D.C.

If you have any questions, please contact Customer Service at 1-800-926-7926 option 1.

Continuing Education Credits

For live event only

In order for us to process your continuing education credit, you must confirm your participation in this webinar by responding to the attendance verification prompts and clicking the link to complete the Certification Process following the webinar.

If you don't click the link following the webinar, you will receive an email including a link to complete the Certification Process within 24 hours.

For any assistance completing the Certification Process, call 1-877-297-2901 or email helpdesk@beaconlive.com. For additional information about continuing education, call us at 1-800-926-7926 option 2.

For live event only

Recording our programs is not permitted. However, today's participants can order a recorded version of this event at a special attendee price. Please call Customer Service at 800-926-7926 option 1 or visit Strafford's website at www.straffordpub.com.

Strafford
A BARBRI Company

OFAC Compliance

Meeting Evolving U.S. Sanctions Requirements, Minimizing Risk of Sanctions

Speakers:
Pete Jeydel, Troutman Pepper Locke
Will Schisa, Davis Polk

August 13, 2025

Agenda

1. **Sanctions overview**
2. OFAC compliance framework and best practices
3. Recent developments
4. Enforcement
5. Violations

U.S. Sanctions: What is OFAC?

The U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") is the primary federal agency administering and enforcing U.S. economic sanctions programs against countries, governments, groups, and individuals

- Purpose is to achieve U.S. national security, foreign policy, or economic goals
- Sanctions generally prohibit U.S. persons (as defined below) from directly or indirectly engaging in or facilitating business with target countries, individuals, or entities.
- Sanctions may be imposed against geographical areas and all persons within those areas, or against designated governments, organizations, individuals, and entities wherever they may be located.
- Sanctions frequently change in response to international events.

The State Department and U.S. Department of Commerce's Bureau of Industry and Security ("BIS") also play a role in administering sanctions.

U.S. Sanctions: Sources of Law

Statutes and executive orders impose sanctions, and OFAC issues regulations to implement them.

- Statutes, executive orders, and regulations, organized by sanctions programs and country, are located on the OFAC sanctions website.

OFAC's regulations use very general language and often are not intuitive.

- Many factual situations will not be addressed directly by clear rules.
- OFAC's interpretation of its regulations is often broader than the language seems.
- Precedent and guidance is often applied across sanctions programs (even if the regulatory language differs).

OFAC provides summaries of sanctions programs on its website; however, where there are ambiguities or nuances in the regulations or summaries, OFAC guidance is minimal.

- OFAC staff may be approached informally, but they are often reluctant to give an opinion without specific and detailed information.
- Request to OFAC for guidance or licenses may only be resolved after many months, if ever.

U.S. Sanctions: Sanctions Programs Building Blocks

Asset Freezes (Blocking)

- Bar transfer of or dealing in property, e.g., assets, liabilities, services, securities, and all contracts in which a sanctions target has any interest (a blocked property interest often is less than legal title or ownership) .

“Sectoral Sanctions”

- Apply to identified entities in certain sectors of the Russian economy
- Prohibit only certain types of transaction (e.g., dealing in new debt or new equity, or supporting certain types of energy projects).

Trade and Investment Embargoes

- Bar imports and/or exports of goods, services (including financial services), and technology.
- Prohibit “new investment” in sanctioned countries/territories

Secondary Sanctions

- Imposed against non-U.S. persons for certain activities completely outside U.S. jurisdiction that involve specific U.S. sanctions targets.

U.S. Sanctions: Jurisdiction

Direct sanctions apply to both U.S. persons and non-U.S. persons acting within U.S. jurisdiction

U.S. sanctions **always** apply to the activities of **U.S. persons** (including employees of non-U.S. companies), which include:

- U.S. entities and their non-U.S. branches
- Non-U.S. subsidiaries of U.S. entities, under Cuba and Iran sanctions only
- U.S. branches and U.S. subsidiaries of non-U.S. entities
- U.S. citizens, including dual citizens and U.S. permanent residents (“green card” holders)
- Persons and entities of any nationality when present or acting in the United States

U.S. sanctions **sometimes** apply to activities of **Non-U.S. persons** within **U.S. jurisdiction**, including any dealings that directly or indirectly involve:

- Participation of U.S. persons
- Actions within the United States (including actions the foreign person causes third parties to take)
- obtaining goods from or services performed in the United States for purposes of the transaction (including U.S. dollar payments)

U.S. Sanctions: Examples of a U.S. Nexus

Recent Enforcement Case: U.S. Dollar Payments

In September 2022, CA Indosuez (Switzerland) S.A. (“CAIS”), agreed to pay $720,258 to settle its potential civil liability for apparent violations of the Cuba, Ukraine-related, Iran, Sudan, and Syria sanctions programs. For approximately three years CAIS operated U.S. dollar banking and securities accounts on behalf of 17 individual customers located in sanctioned jurisdictions and conducted U.S. dollar business on behalf of these customers through the U.S. financial system, including through U.S. correspondent banks and U.S. registered brokers or dealers in securities. Although CAIS itself was not a U.S. person, the transactions touching the U.S. financial system established U.S. jurisdiction.

Recent Enforcement Case: “Causing” a Violation

In 2022, Sojitz (Hong Kong) Limited, a Hong Kong-based company that engages in offshore trading and cross-border trade financing, agreed to pay $5.2 million for violations of Iranian sanctions regulations. Sojitz allegedly made U.S. dollar payments through U.S. financial institutions for Iranian-origin resin from its bank in Hong Kong to the resin supplier’s banks in Thailand. In doing so, Sojitz “caused” the U.S. financial institutions that processed the funds to engage in and facilitate prohibited financial transactions related to goods of Iranian origin. Sojitz was liable for causing this violation, and was subject to U.S. jurisdiction, even though its conduct took place outside of the United States.

U.S. Sanctions: Facilitation

Most U.S. sanctions programs also prohibit U.S. Persons from "facilitating" transactions by non-U.S. Persons that would be prohibited for a U.S. Person to conduct.

- For example, a U.S. Person cannot assist a non-U.S. affiliate in engaging in a prohibited transaction with an SDN.
- OFAC regulations do not provide a definition for "facilitation," but it is interpreted broadly.
  - A U.S. Person cannot assist or approve a prohibited transaction by a foreign entity.
  - A U.S. parent company may not alter its operating procedures specifically to enable a foreign subsidiary to deal with sanctioned persons.
  - A U.S. parent company may not refer prohibited transactions to any foreign person.
  - "Facilitation" can also include business and legal planning; decision-making; approvals; designing; ordering or transporting goods; or providing financial or insurance assistance.
  - Purely clerical and reporting services are generally not considered "facilitation."
- U.S. persons are also prohibited from engaging in activities intended to evade or avoid sanctions prohibitions.

Agenda

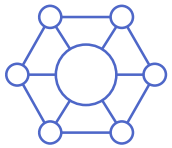
1. Sanctions overview
2. **OFAC compliance framework and best practices**
3. Recent developments
4. Enforcement
5. Violations

OFAC’s Compliance Framework

Identifies five essential elements of an effective Sanctions Compliance Program (SCP)

Senior Management Commitment

Risk Assessment



Internal Controls

Testing and Auditing

Training

Elements of an Effective SCP

Senior Management Commitment

- Senior management should review and approve SCP; ensure compliance function has adequate resources and autonomy, and promote a culture of compliance.

OFAC Risk Assessment

- Companies must conduct a periodic risk assessment that analyzes risks posed by clients and customers, products, services, supply chain, intermediaries, counter-parties, transactions, and geographic locations.

Internal Controls

- Companies should maintain policies, procedures, and internal controls that are tailored to their risk profile and allow the company to identify, interdict, escalate, report (as appropriate), and keep records pertaining to activity that is prohibited by the sanctions programs administered by OFAC.

Testing and Auditing

- Companies should ensure the effectiveness of their SCP through testing/audit. Function should be comprehensive, independent, and objective. Negative results should be promptly addressed.

Training

- Companies should provide training to all appropriate employees, based on nature of business and sanctions risk. Targeting training should be refreshed on a periodic basis (at least annually).

Compliance Expectations

OFAC expects risk-based compliance

- SCP Framework re-emphasizes OFAC's risk-based approach, based on:
  - Size and sophistication
  - Customers and counterparties
  - Products and services
  - Geographic locations

Agenda

1. Sanctions overview
2. OFAC compliance framework and best practices
3. **Recent developments**
4. Enforcement
5. Violations

Extended SOL and recordkeeping requirement

Extended recordkeeping requirements become effective

- In 2024, the statute of limitations for violations of IEEPA and the Trading with the Enemy Act was extended from five years to 10 years, and OFAC issued an interim final rule extending recordkeeping requirements accordingly
- Extension to record retention requirements became effective through a final rule on March 12, 2025. Persons engaged in transactions subject to OFAC sanctions programs must now maintain records for a period of 10 years

New administration: Sanctions policy agenda

The second Trump administration has aggressively leveraged sanctions, secondary sanctions, and a broad range of other authorities to support its foreign policy goals

- Novel uses of the International Emergency Economic Powers Act (**IEEPA**) to impose not only primary sanctions but also sweeping tariffs and threatened "secondary tariffs"
- "Maximum pressure" approach against foreign governments to support policy goals (e.g., Iran)
- Threat of secondary sanctions and tariffs to pressure third-party countries trading with sanctioned states and governments (notably Russia, Iran, Venezuela)
- Heightened focus on cartels and transnational criminal organizations, including through foreign terrorist organization (**FTO**) designations
- Decreased emphasis on international coordination, in support of "America First" policy
- Businesses face a rapidly evolving compliance environment, with a need for adaptable programs to address novel measures

Sanctions Program Developments

- Iran – return to maximum pressure (potential “JCPOA 2.0”?)
- Russia – outlook TBD
- China – no major developments (loud calls for action on the Hill)
- Syria – sanctions largely lifted
- Cuba – revocation of limited 11th hour sanctions relief
- Venezuela – back and forth and back again on critical oil sector sanctions
- Yemen/Houthis – FTO designation, revocation of authorizations
- Israel – termination of West Bank sanctions
- New (again) ICC sanctions

Targeting of cartels and transnational criminal organizations

The Administration has directed the federal government to pursue the "total elimination of cartels" through sanctions and other measures

- A January 2025 E.O. ordered the Secretary of State to designate eight major cartels and transnational criminal organizations as FTOs and Specially Designated Global Terrorists (**SDGTs**)
  - Corollary DOJ memo directs resources towards prosecution of designated cartels, including use of "material support" laws to target third parties dealing with cartels
- OFAC has targeted financial facilitators and money laundering networks for cartels, including entities operating bulk cash smuggling and repatriation schemes
- Efforts closely coordinated among government agencies and law enforcement
  - Financial Crimes Enforcement Network (**FinCEN**) issued statements, guidance, and orders to increase scrutiny of cross-border transactions and financial institutions linked to illicit activity
- Businesses with exposure to Mexico and Latin America face an increasingly complex risk landscape (although enforcement to date has focused on cartels and non-U.S. entities)

Impacts of cartel terrorist designations

On February 20, State and Treasury designated eight cartels as FTOs and SDGTs.

- Impacts
  - Material support crime
  - Blocking property of “agents”
- Related actions by FinCEN
  - “Special measures” imposed under the FEND Off Fentanyl Act on three financial institutions in Mexico (“primary money laundering concern”)
  - GTO: $200 reporting threshold (CTRs/MSBs)
  - Guidance on Mexico oil smuggling

Sanctions and AML

- **Trump administration seeking to reduce BSA/AML regulatory burdens**
  - Regulatory rollbacks (e.g., CTA beneficial ownership information reporting rule, investment adviser rule)
  - Focus on supporting innovation (e.g., crypto, fintech).
- **GENIUS Act and new compliance framework for regulated payment stablecoin issuers**
- **Questions about DeFi (e.g., Tornado Cash delisting)**
- **Opposition to “debanking”**

Potential further changes to AML/CFT framework

The Administration may revisit and amend or withdraw other Biden-era AML/CFT rules

- In June 2024, FinCEN and the federal banking agencies issued proposed rules that would amend AML/CFT program requirements under the BSA and explicitly require financial institutions to establish "effective, risk-based, and reasonably designed" AML/CFT compliance programs (the **Proposed AML/CFT Program Rule**)
  - The Proposed AML/CFT Program Rule is being reevaluated under the new administration; in practice, it would expand the compliance burdens of financial institutions
  - Final rule may be used as an opportunity to significantly reduce BSA compliance obligations

Convergence with export controls compliance

On October 9, 2024, BIS issued new guidance for financial institutions on best practices for compliance with export control laws and regulations (the Guidance)

- The Guidance followed numerous alerts from BIS and other regulators on EAR compliance expectations for financial institutions and a BIS final rule tightening its voluntary self-disclosure (**VSD**) and enforcement guidelines
- Guidance focuses on compliance obligations under the EAR's General Prohibition 10
- Sets out highly prescriptive requirements for financial institutions to monitor for violations of export control laws and significantly expands traditional compliance expectations
  - Expectations include real-time screening of transactions, due diligence at onboarding, and processes to halt and investigate transactions linked to export control violations
- No further guidance has been released to date, but financial institutions are expected to take a risk-based approach to implementing controls

Agenda

1. Sanctions overview
2. OFAC compliance framework and best practices
3. Recent developments
4. **Enforcement**
5. Violations

Enforcement and Penalties

The penalties for violations can be substantial. Depending on the program:

- Civil penalties can range from a maximum of $111,308 to $1,876,699 per violation
  - Civil violations are enforced by OFAC.
  - Civil violations of sanctions are strict liability and can occur even if a person has no actual knowledge of the violation.
- Most cases are covered by the International Emergency Economic Powers Act ("IEEPA"), authorizing a civil penalty that is the greater of $377,700 per violation (periodically adjusted for inflation) or twice the value of the transaction.
- Criminal penalties for willful violations can include fines ranging from $50,000 to $10,000,000 and imprisonment ranging from 10 to 30 years.
  - Criminal violations are enforced by the Justice Department.
- OFAC's actual enforcement generally focuses on willful violations and cases in which the violator had reason to know of a potential violation (or the risk of one).

How are U.S. Sanctions Enforced?

Civil Enforcement

- OFAC weighs its enforcement response and calculates any monetary penalties under the general factors set out in its Economic Sanctions Enforcement Guidelines.
  - Among other factors, OFAC will consider the "existence, nature and adequacy of a [company's] risk-based OFAC compliance program at the time of the apparent violation" in determining what enforcement response is warranted.
  - OFAC also weighs the remedial response to apparent violations, including whether the company put in place an OFAC compliance program where none existed or, where a program did exist, if the company "took appropriate steps to enhance the program to prevent the recurrence of similar violations."
  - Potential OFAC responses range from taking no action to cautionary letters and findings of violations (including penalties).
- Severity of any monetary penalties turns on whether or not OFAC determines the violation was "egregious" and whether or not the parties self-disclosed the violation to OFAC
  - "Self-disclosure can result in as much as a 50% discount on otherwise applicable civil monetary penalties."
- **Most OFAC investigations are resolved through non-public actions without a penalty.**

How are U.S. Sanctions Enforced?

The DOJ aggressively enforces criminal violations of U.S. sanctions

- **Criminal liability** possible for willful misconduct
  - In order to find willful misconduct, defendants must act with knowledge that their conduct was unlawful (i.e., not by mistake or negligence)
  - DOJ can also bring related charges (bank fraud, money laundering, conspiracy)
- **Forfeiture**
  - U.S. authorities may seek forfeiture of any property, real or personal, that is or is derived from the proceeds traceable to a violation of sanctions under 18 U.S.C. § 981 or 28 U.S.C. § 2461

DOJ Sanctions Enforcement Developments

- **DOJ has disbanded:**
  - Corporate Enforcement Unit
  - Task Force KleptoCapture
  - Kleptocracy Asset Recovery Initiative
  - National Cryptocurrency Enforcement Team
- **But expect tough enforcement to continue**

DOJ Criminal Enforcement Priorities

Stated priorities of new administration, as set forth in DOJ Criminal Division's May 2025 memo include sanctions and AML

U.S. Department of Justice

Criminal Division

Office of the Assistant Attorney General *Washington, D.C. 20530*

May 12, 2025

MEMORANDUM

TO: All Criminal Division Personnel

FROM: Matthew R. Galeotti
Head of the Criminal Division

SUBJECT: Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime[1]

B. Prioritization and Associated Policy Changes

To combat these harms, the Criminal Division will prioritize investigating and prosecuting white-collar crimes in the following high-impact areas:

Conduct that threatens the country's national security, including threats to the U.S. financial system by gatekeepers, such as financial institutions and their insiders that commit sanctions violations or enable transactions by Cartels, TCOs, hostile nation-states, and/or foreign terrorist organizations;

Complex money laundering, including Chinese Money Laundering Organizations, and other organizations involved in laundering funds used in the manufacturing of illegal drugs;

Bribery and associated money laundering that impact U.S. national interests, undermine U.S. national security, harm the competitiveness of U.S. businesses, and enrich foreign corrupt officials;[6] and

As provided by the Digital Assets DAG Memorandum: crimes (1) involving digital assets that victimize investors and consumers; (2) that use digital assets in furtherance of other criminal conduct; and (3) *willful* violations that facilitate significant criminal activity.

Enforcement focus: Individuals

DOJ guidance continues to emphasize primary focus on individuals

> *"The Department's first priority is to prosecute individual criminals. It is individuals—whether executives, officers, or employees of companies—who commit these crimes, often at the expense of shareholders, workers, and American investors and consumers. The Criminal Division will investigate these individual wrongdoers relentlessly to hold them accountable."*
>
> **– DOJ Criminal Division May 12, 2025 Memo**

Multiple OFAC actions brought against individuals

- Intentional evasion of U.S. financial institutions
- Knowingly processing transactions for blocked individual
- Transferred nominal ownership from SDNs to non-sanctioned family members with no or minimal consideration

Other enforcement themes

Effective compliance program critical to mitigating sanctions and AML risk	– Controls should test for potential technical failures – Controls should cover entire lifecycle of transactions – Compliance program should be sufficiently resourced
Broad jurisdictional bases for bringing actions	– Non-U.S. companies “causing” U.S. financial institutions to process transactions for sanctioned persons – Continued scrutiny of foreign subsidiaries of U.S. companies
Scrutiny of M&A-related conduct	– First declination brought under DOJ National Security Division’s M&A policy – Acquirer liable to OFAC for pre-acquisition violations
Focus on gatekeepers, including financial institutions and service providers	– VC firm worked with SDN’s nephew and various legal entities, that were all acting as proxy for SDN – Real estate broker assisted two sanctioned individuals in hiding ownership interest in luxury condos

Agenda

1. Sanctions overview
2. OFAC compliance framework and best practices
3. Recent developments
4. Enforcement
5. **Violations**

Voluntary Self-Disclosure

A voluntary self-disclosure ("VSD") can result in as much as a 50% reduction in penalties.

- Filing a VSD is never required, and whether it is appropriate is a question of judgment. In general, most sophisticated institutions do not report every potential sanctions violation to OFAC.
- Most sophisticated institutions make risk assessments of the significance of potential violations and weigh that against the institutional and governmental resources required to make and process the relevant reports.
  - As a general matter, a VSD should be seriously considered where an apparent violation may have caused significant harm, involved actual knowledge or intentional misconduct, or identifies a systemic weakness or problem.
  - Trivial VSDs simply add to OFAC's caseload without creating any policy or enforcement value.
- For most sophisticated institutions, the two principal considerations are: (1) whether an enforcement is a realistic possibility (and the VSD would mitigate potential consequences); and (2) whether the VSD might provide valuable intelligence to law enforcement.
- In all cases (regardless of whether a VSD is filed), OFAC expects institutions to take appropriate remedial action.
- The usual timeline for a VSD after filing is weeks to months.

Factors to Consider in Filing a VSD

The decision to file a VSD is always a fact-sensitive question. In general, relevant considerations include:

- **Knowledge of Conduct**: The degree to which an organization's personnel knew of, or had reason to know of, the risk of a violation.
- **Role in the Transaction**: Organization's relationship to the underlying sanctions target, ranging from scenarios in which there is no direct relationship to the sanctions target (e.g., the target is the client of a client or of another downstream institution) to scenarios in which there is a direct relationship.
- **Sanctions Harm**: The nature and seriousness of the potential violation from a policy perspective.
- **Volume/Value of Transactions**: The number and volume of the transactions that took place and the total value of the underlying transactions.
- **Control Effectiveness**: The degree to which internal controls could have detected or prevented the violation (or should have done so) and the extent to which the potential violation indicates systemic weaknesses or control failures.
- **Value of Information to OFAC**: The extent to which it appears likely that the information is already otherwise known to or readily identified by OFAC or U.S. law enforcement authorities.

Potential Outcomes of a VSD

Possible administrative responses to a VSD include:

- **No-Action Letter:** OFAC issues no-action letters in circumstances where it does not believe that sanctions have been violated. These can provide useful information where the institution is uncertain how OFAC would view a particular rule or set of facts, but essentially the no-action letter tells the institution that there was in fact nothing to disclose.
- **Cautionary Letter:** This is by far the most common resolution of VSDs, constituting the overwhelming majority of the 90%+ of cases in which there is a VSD but OFAC does not take public enforcement action. The cautionary letter indicates that OFAC agrees that a violation of sanctions likely took place or that conduct occurred that could result in future violations, but it does not believe that public enforcement action against the reporting institution is appropriate.
- **Enforcement Action:** In a small minority of cases, OFAC takes further action following the VSD. This may include requests for additional information or administrative subpoenas (which do not preclude closing the investigation via letter without a penalty) and, ultimately, a request for a proposal for a settlement or a notice of proposed penalty.
  - It is possible for OFAC to make a criminal referral, but this is extremely rare (although criminal authorities may open an investigation once the underlying issues become public).

Updates to DOJ's Corporate Enforcement and Voluntary Self-Disclosure Policy ("CEP")

Previous Policy

- Meeting CEP requirements relating to self-disclosure, cooperation, and remediation absent aggravating circumstances creates *presumption* of a declination
- If aggravating circumstances present, declination only possible if "immediate" disclosure, "extraordinary" cooperation and remediation, and effective preexisting compliance program

New Policy

- Meeting CEP requirements relating to self-disclosure, cooperation, and remediation absent aggravating circumstances *requires* declination
- If aggravating circumstances are present, prosecutors have discretion to recommend declination
- "Near miss" situations (self-reporting that does not qualify as voluntary self-disclosure or presence of certain aggravating factors) specifically contemplated for specified resolutions.

Contact

Pete Jeydel

Partner, Troutman Pepper Locke
Office: Washington DC
Phone: 202.274.2962
Peter.Jeydel@troutman.com

Will Schisa

Counsel, Davis Polk
Office: Washington DC
Phone: 202.962.7129
will.schisa@davispolk.com

Q&A

You may use the Chat function to ask questions or email questions to **intlaw@straffordpub.com**.

Group Listening Code: TLLQTA

Please watch for

The Certification Process link to appear on your screen to complete the survey and request your certificate(s).

Try the CLE Individual Annual Pass

Not a Passholder Yet?

- Attend unlimited live webinars in any of our legal practice areas — we produce over 750+ advanced live CLE webinars each year
- Get unlimited access to hundreds of recorded webinars
- Get all your CLE credits for one price
    - Simply respond to the email you will receive after the program and we will rebate the cost of this webinar from the pass price!

- Did you know that Strafford offers volume discounts? Add additional attendees to your next webinar order at 35% off (40% off for 5 or more).