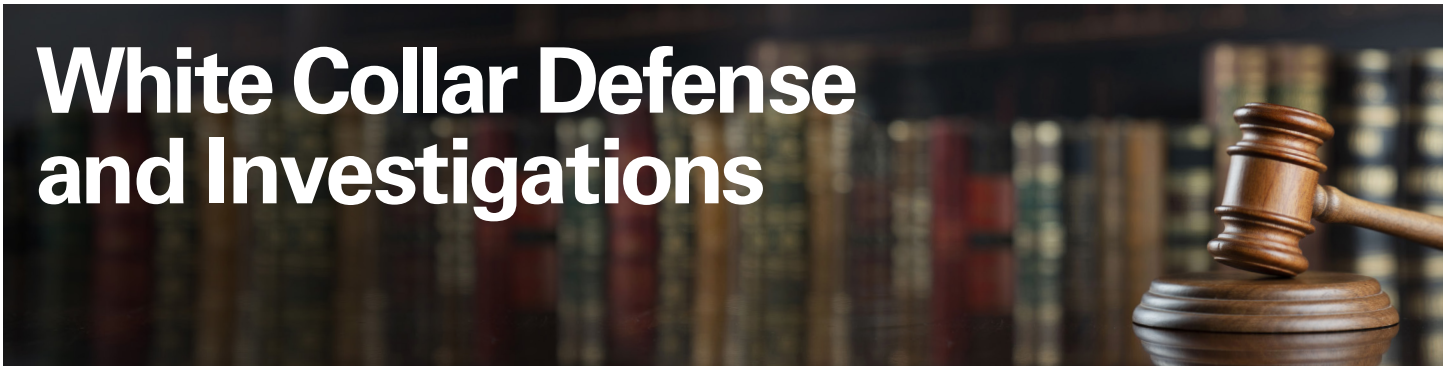
March 16, 2023

Skadden

White Collar Defense and Investigations



If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
1.212.735.3000

1440 New York Avenue, N.W.
Washington, D.C. 20005
1.202.371.7000

22 Bishopsgate
London EC2N 4BQ
44.20.7519.7000

New US Efforts To Prosecute Sanctions Evasion and Export Control Violations May Require Compliance Programs To Be Updated

Takeaways

- The U.S. government is putting new emphasis on investigating and prosecuting those who evade sanctions and export control rules — moves that may require some companies to reassess their compliance programs.
- The Department of Justice is assigning more resources to investigate and prosecute violations, and it issued joint guidance with Treasury and Commerce Departments to assist in spotting the use of third-party intermediaries and transshipment points to evade Russia-related sanctions and export controls.
- Financial institutions and companies engaged in international trade should ensure that their compliance programs are risk-based and dynamic in response to the novel and expansive use of sanctions and export controls against Russia and new methods of evasion.
- If a business finds that it may have violated sanctions or export controls, it should consider whether to self-report in order to take advantage of the government's policy of mitigating penalties for those who report their own violations.

DOJ Increases Resources To Investigate and Prosecute Sanctions Evasion and Export Control Violations

On March 2, 2023, during a keynote speech at the American Bar Association's annual White Collar Crime National Institute, Deputy Attorney General (DAG) Lisa Monaco identified sanctions as "the new FCPA" (Foreign Corrupt Practices Act) and announced that significant new resources would be devoted to addressing the "troubling trend" of the intersection of corporate crime and national security.[1]

DAG Monaco revealed plans to enhance the National Security Division (NSD) by adding more than 25 prosecutors and hiring its first-ever chief counsel for corporate enforcement. DAG Monaco also announced a "substantial investment" in the Criminal Division's Bank

[1] This client alert is for informational purposes only and does not constitute legal advice. Complex assessments often have to be made as to which sanctions regime applies in any given instance, given the multinational touch points of many entities and individuals. In that regard, given the complex and dynamic nature of these sanctions regimes, there may be developments not captured in this summary. Moreover, while the summary was accurate when written, it may become inaccurate over time given developments. For all of these reasons, you should consult with a qualified attorney before making any judgments relating to sanctions, as there are potentially severe consequences of failing to adhere fully to sanctions restrictions.

New US Efforts To Prosecute Sanctions Evasion and Export Control Violations May Require Compliance Programs To Be Updated

Integrity Unit to build upon its track record of prosecuting global financial institutions for international money laundering and sanctions evasion and bolster its partnership with the NSD. These initiatives follow the February 16, 2023, announcement of the creation of a Disruptive Technology Task Force to target illegal transfers of sensitive technologies to Russia and other countries of concern.

DOJ, Commerce and Treasury Issue Joint Compliance Note on Russia-Related Sanctions and Export Controls

On the same day as DAG Monaco's speech, the Departments of Commerce and Treasury and DOJ issued their first-ever "Tri-Seal Compliance Note" warning financial institutions and multinational companies that the U.S. government is "cracking down" on the use of third-party intermediaries and transshipment points to evade Russian-related sanctions and export controls.

The joint compliance note includes a list of common "red flags" suggesting that a third party may be engaged in efforts to evade sanctions or export controls. It also advises financial institutions and companies to review civil enforcement and targeting actions by Department of Commerce's Bureau of Industry and Security (BIS) and the Department of the Treasury's Office of Foreign Assets Control (OFAC), as well as indictments obtained by the Department of Justice.

What Should Businesses Do in Response?

Financial institutions and companies engaged in international trade should ensure that their compliance programs are appropriately designed, tested and resourced to address the increased risk of violations stemming from the novel and expansive sanctions and export controls implemented by the U.S., EU, U.K. and other countries against Russia.

- **Maintain and update an effective risk-based sanctions and export control compliance program**

  Consistent with OFAC's prior guidance from May 2019, the joint compliance note identifies the five key components of an effective, risk-based sanctions and export compliance program (SECP) including: (1) management commitment, (2) risk assessment, (3) internal controls, (4) testing and auditing and (5) training. An SECP must also be dynamic and, in light of the evolving geopolitical landscape, compliance personnel should be trained to regularly consult guidance and advisories from Treasury and Commerce to inform and strengthen their compliance programs.

  Entities should strengthen controls targeted at third-party risks, particularly in geographies with known nexuses to Russia and Belarus. The joint compliance note specifically calls out risks related to (1) third parties posing as end customers who are in fact intermediaries engaged to obscure the identities of Russian end-users; and (2) use of transshipment points to circumvent restrictions and facilitate the movement of restricted goods to Russia, including items of heightened concern such as microelectronics.

  Financial institutions and other companies should train employees in sales and operational roles who own and manage operational risk (the "first line of defense" in most compliance programs), to identify patterns associated with third-party intermediaries seeking to circumvent restrictions. The joint compliance note sets out a non-exhaustive list of red flags to assist entities with early detection including:

  1. Use of corporate entities that obscure ownership, source of funds or countries involved in a transaction.
  2. A customer's reluctance to share information about end use of a product, including reluctance to complete an end-user form.
  3. Use of shell companies to conduct international wire transfers.
  4. Declining customary installation, training or maintenance of the purchased item(s).
  5. Internet protocol (IP) addresses that do not correspond to a customer's reported location data.
  6. Last minute changes to shipping instructions that appear contrary to customer history or business practice.
  7. Payment from a third party or business not listed on the end-user form.
  8. Use of personal email accounts instead of company email addresses.
  9. Operation of complex and/or international businesses using residential addresses, or addresses common to multiple closely-held corporate entities.
  10. Changes to standard letters of engagement that obscure the ultimate customer.
  11. Transactions involving a change in shipments or payments that were previously scheduled for Russia or Belarus.
  12. Transactions involving entities with little or no web presence.
  13. Routing purchases via certain transshipment points (China, Hong Kong and Macau) and jurisdictions close to Russia, including Armenia, Turkey and Uzbekistan.

  The joint compliance note also notes that complex sales and distribution models may hinder visibility into the ultimate end-users.

  When a company detects warning signs of potential sanctions evasion or export control violations, it is essential to move quickly to conduct additional due diligence and exercise heightened caution while doing that. Compliance personnel should establish

a framework for documenting additional due diligence results, including reasons for discontinuing a business relationship, or continuing one with additional safeguards, such as enhanced due diligence measures. Companies with existing anti-corruption and/or anti-money laundering frameworks can leverage those resources to prioritize risk areas.

- **Develop procedures for screening customers and counterparties through the Consolidated Screening List**

  A best practice in the face of evolving sanctions evasion and export control risk is to screen not only customers but also intermediaries and counterparties through the U.S. government's Consolidated Screening List, which includes all of the sanctions- and export controls-restricted party lists maintained by OFAC and BIS.

  While companies need not adopt a "one size fits all" approach to potential matches, given the differences in the various lists, it is essential to have procedures in place to identify and take appropriate action to address potential matches. Screening should capture both new and existing relationships, and must be updated regularly. The priority and frequency of screening should be consistent with the company's assessment of potential risks, and appropriate resources should be devoted to the process.

- **Conduct additional risk-based due diligence on customers, intermediaries and counterparties**

  Effective risk assessment requires companies to identify sanctions and export controls risk posed by: (1) the nature and sensitivity of the company's operations, products or services, (2) the geographies of the company's operations and customers and (3) third parties, including customers, counterparties and intermediaries.

  Financial institutions and companies must regularly assess and revise compliance measures to account for evolving evasion tactics as well as operational changes in their business, such as acquisition of a new foreign subsidiary or an expansion of distribution territories. They should also ensure that any updated measures, tactics and typologies are communicated down to the first line of defense — the functions that own and manage risk.

- **Monitor BIS and OFAC enforcement actions and DOJ indictments, which describe new tactics and methods used to evade sanctions and export controls**

  OFAC's recent civil enforcement actions flag recurring tactics, including use of front companies, falsification of transactional documents, omission of key information from internal correspondence and shipment of goods from third countries. The joint compliance note highlighted several administrative enforcement actions involving intermediaries and transshipment points, including a substantial penalty imposed by BIS on a U.S. company for shipping integrated circuit components, which are critical components in missiles and military satellites, to Russia via a Bulgarian front company.

  Evasion tactics identified in recent DOJ indictments include:

  1. Using shell companies located in third countries as intermediaries or purported end users: In one case, DOJ alleges that only one of the five intermediary parties had any visible signage and its place of business consisted of an empty room in a strip mall.
  2. Claiming that items would be used by entities engaged in activities subject to less stringent oversight: On at least one occasion, a defendant allegedly claimed that an item would be used by Russian space program entities, when in fact the item was suitable for military aircraft or missile systems only.
  3. Dividing shipments of controlled items into multiple, smaller shipments to try to avoid law enforcement detection.
  4. Using aliases for the identities of the intermediaries and end users.
  5. Transferring funds from shell companies in foreign jurisdictions into U.S. bank accounts and quickly forwarding or distributing funds to obfuscate the audit trail or the foreign source of the money.
  6. Making false or misleading statements on shipping forms, including underestimating the purchase price of merchandise by more than five times the actual amount.
  7. Claiming to do business not on behalf of a restricted end user but rather on behalf of a U.S.-based shell company.

  Reinforcing the findings of the joint compliance note, on March 9, 2023, the multilateral Russian Elites, Proxies and Oligarchs (REPO) Task Force issued its first Global Advisory on Russian Sanctions Evasion. It also sets out typologies of Russian sanctions evasion, including use of intermediaries and transshipment points. Notably, it also flags the frequent use of family members and close associates to ensure continued access and control of assets after the imposition of sanctions, and the use of real estate as a vehicle for holding and maintaining Russian wealth.

- **Implement policies and foster a culture that strongly encourages escalation and internal reporting of potential violations**

  Effective compliance programs should empower and protect employees who identify and report potential sanctions and exports control violations to compliance personnel or management.

Companies should also consider how to incentivize executives and managers to focus on the SECP in light of the DOJ Criminal Division's pilot program to require, as part of any criminal resolution, that corporate compliance programs include compensation-related provisions.

U.S. Agencies Urge Voluntary Self-Disclosures

The joint compliance note urges parties who may have violated sanctions or export controls to conduct internal investigations and make timely voluntary self-disclosures to OFAC, BIS and the NSD's Counterintelligence and Export Control Section. Generally speaking, none of the agencies offer a complete amnesty but each offers some potential mitigation of penalties for self-reporting violations.

The submission of a disclosure to OFAC does not preclude the imposition of a civil or administrative penalty, but OFAC's penalty guidance establishes mitigation of up to 50% of the base penalty as the starting point for any violation involving a disclosure.

BIS strongly encourages disclosure of potential violations of the Export Administration Regulations (ERA) or any order or license issued thereunder to the Office of Export Enforcement (OEE). Voluntary self-disclosure is a mitigating factor in OEE's determination of administrative sanctions, but is considered together with all factors in a case and may be outweighed by aggravating factors. Additionally, the BIS regulations make clear that voluntary self-disclosure does not preclude referral by the OEE to the DOJ for potential criminal prosecution.

In cases of intentional or willful violations (*i.e.*, with knowledge that the conduct is unlawful), a party seeking to take advantage of NSD's voluntary self-disclosure policy must self-report to NSD directly and cannot rely on self-disclosures to OFAC or BIS alone. The DOJ has focused heavily on incentivizing self-reporting in recent policies and speeches, offering clear and significant benefits for companies that do so.

If a company voluntarily self-discloses potentially criminal violations to NSD, fully cooperates (including provision of all non-privileged information and identification of relevant individuals) and timely and appropriately remediates the criminal conduct (including agreeing to pay all disgorgement, forfeiture and restitution resulting from the misconduct), absent aggravating factors, NSD generally will not seek a guilty plea, and there is a presumption that the company will receive a non-prosecution agreement and will not pay a fine. The NSD also has discretion to issue a declination.

For more information on self-reporting, see our January 19, 2023, alert "DOJ Doubles Down on Efforts to Incentivize Early Self-Reporting and Cooperation" and our March 3, 2023, alert, "DOJ Implements Voluntary Self-Disclosure Policy for U.S. Attorneys' Offices."

New US Efforts To Prosecute Sanctions Evasion and Export Control Violations May Require Compliance Programs To Be Updated

Contacts

Maria Cruz Melendez
Partner / New York
212.735.2320
maria.cruzmelendez@skadden.com

Jack P. DiCanio
Partner / Palo Alto
650.470.4660
jack.dicanio@skadden.com

Brian J. Egan
Partner / Washington, D.C.
202.371.7270
brian.egan@skadden.com

Alessio Evangelista
Partner / Washington, D.C.
202.371.7170
alessio.evangelista@skadden.com

Eytan J. Fisch
Partner / Washington, D.C.
202.371.7314
eytan.fisch@skadden.com

Steven R. Glaser
Partner / New York
212.735.2465
steven.glaser@skadden.com

Andrew M. Good
Partner / London
44.20.7519.7247
andrew.good@skadden.com

Ryan D. Junck
Partner / London
44.20.7519.7006
ryan.junck@skadden.com

Bradley A. Klein
Partner / Washington, D.C.
202.371.7320
bradley.klein@skadden.com

Steve Kwok
Partner / Hong Kong
852.3740.4788
steve.kwok@skadden.com

David Meister
Partner / New York
212.735.2100
david.meister@skadden.com

Khalil N. Maalouf
Counsel / Washington, D.C.
202.371.7711
khalil.maalouf@skadden.com

Bora P. Rawcliffe
Counsel / London
44.20.7519.7139
bora.rawcliffe@skadden.com

Pippa Hyde
Associate / London
44.20.7519.7193
pippa.hyde@skadden.com