Skadden

Alessio Evangelista and Eytan Fisch are partners, Khalil Maalouf is counsel and Alyssa Domino is a law clerk at Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates. Mr Evangelista can be contacted on +1 (202) 371 7170 or by email: alessio.evangelista@skadden.com. Mr Fisch can be contacted on +1 (202) 371 7314 or by email: eytan.fisch@skadden.com. Mr Maalouf can be contacted on +1 (202) 371 7711 or by email: khalil.maalouf@skadden.com. Ms Domino can be contacted on +1 (202) 371 7139 or by email: alyssa.domino@skadden.com

Published by Financier Worldwide Ltd

SPECIAL REPORT ARTICLE REPRINT February 2024

US government agencies raise the bar on national security-related corporate compliance

BY ALESSIO EVANGELISTA, EYTAN FISCH, KHALIL MAALOUF AND ALYSSA DOMINO

The ongoing war in Ukraine, armed conflict in the Middle East, rising geopolitical tension between the US and China, and the continuing evolution of the digital assets ecosystem, have caused US federal government agencies to add and redirect enforcement resources toward combatting money laundering, terrorist financing, sanctions evasion and export control violations. These efforts are government-wide and include releasing detailed multi-agency compliance guidance, proposing and promulgating new rules and regulations, stepping up enforcement, and hiring additional staff.

Companies and financial institutions (FIs) can manage the resulting compliance and enforcement risks by refreshing their risk assessments, addressing deficiencies identified by independent assessments, and ensuring that guidance published by government agencies has been adequately incorporated into their compliance programmes. Companies and FIs should also act quickly when potential violations of these rules are discovered. And in some instances, companies may want to take advantage of several newly enhanced voluntary self-disclosure programmes across the US government.

Compliance alerts

The multi-agency compliance alerts issued in 2023 were both educational tools and warning shots signalling that companies and FIs should expect increased scrutiny and potentially significant penalties if their compliance programmes are weak or ineffective.

Most recently, on 11 December 2023, the Departments of Commerce, Treasury, Justice, State and Homeland Security released a 'Quint-Seal Compliance Note' that identified best practices for the safe and compliant transport of goods in maritime and other forms of transportation. The agencies pointed out tactics that malign actors use to avoid US sanctions and export controls, both to help companies enhance their compliance programmes and to signal that the US government is closely watching for corporate compliance in this arena.

While the Quint-Seal guidance was notable for involving five agencies, different

constellations of agencies have issued joint guidance regularly over the past year. For example, on 6 November 2023, the Financial Crimes Enforcement Network (FinCEN) and the Bureau of Industry and Security (BIS) issued their third joint alert urging FIs to be vigilant against efforts by individuals and entities to evade export controls administered by BIS. This alert highlighted a new suspicious activity report (SAR) key term that FIs were directed to use when they report potential efforts to evade US export controls beyond the Russia-related circumstances that were the focus of two prior alerts on 28 June 2022 and 19 May 2023.

Similarly, a 26 July 2023 joint compliance note released by the Department of Justice's (DOJ's) National Security Division (NSD), BIS and the Treasury's Office of Foreign Assets Control (OFAC) discussed the benefit of making voluntary self-disclosures as a tool to reduce the risk of enforcement and mitigate civil or criminal liability. This 'Tri-Seal Compliance Note' also highlighted the availability of significant monetary awards for whistleblowers who provide information about sanctions and export control violations.

The compliance alerts provide compliance tips, ranging from steps to prevent funding streams for terrorist organisations to highlighting the risks posed by the use of convertible virtual currency (CVC) mixing services by a variety of threat actors. They simultaneously provide a compliance roadmap for companies while demonstrating that the federal government is focused on compliance with the expectation that companies take action to protect themselves against the multitude of risks in these areas.

Adapting to changing rules and regulations

In addition to providing guidance through compliance alerts, the federal government continues to issue new rules and regulations to promote compliance. For example, agencies have continued to raise the bar on corporate diligence expected of companies that do business in the US. The Corporate Transparency Act (CTA), which aims to combat illicit activity, including money laundering and terrorism financing, became effective on 1 January 2024, with a suite of regulations designed to require companies in the US to report detailed beneficial ownership information to FinCEN. Although 23 types of entities are exempt from the CTA's reporting requirements – including securities reporting issuers, banks, registered investment advisers, large operating companies and subsidiaries of certain exempt entities – millions of US entities and non-US entities registered to do business in the US will be subject to filing requirements.

In another development, in October 2023 FinCEN issued a 'Notice of Proposed Rulemaking' that would require domestic FIs and agencies to adopt new recordkeeping and reporting requirements for transactions involving CVC mixing. This was the first time since 2018 that a new proposed rule relying on section 311 of the Patriot Act was issued, and the first ever targeting of a class of transactions as opposed to a specific entity or country.

Additionally, in the same month, BIS released a package of rules designed to update export controls on advanced computing semiconductors and semiconductor manufacturing equipment. These rules impose licensing requirements for US persons who seek to export semiconductor manufacturing equipment to any of approximately 40 countries. They also impose end-use controls for companies dealing in semiconductors whose ultimate parents are located in China or certain other countries where licensing requirements now exist. Companies should assess the impact of these restrictions on their activities, both domestically and internationally, and ensure that their compliance programmes incorporate the new recordkeeping and reporting requirements.

The US government has also broadened sanctions against numerous targets, with a particular focus on Russia. For example, in December 2023, President Biden issued a new executive order (EO) expanding sanctions targeting Russia's military-industrial base and tightening restrictions on imports into the US of certain Russia-origin goods. The EO was the latest in a series of coordinated actions whereby the US expanded and strengthened enforcement of its sanctions and export controls against Russia. In November, OFAC issued nearly 100 sanctions that chiefly targeted Russia's defence procurement and mining sectors. In October and November, OFAC issued sanctions on vessels and their owners for violations of Russia's oil price cap regime. And in May, OFAC, the State department and BIS imposed sweeping Russia-related sanctions and export controls, and BIS issued a supplemental joint alert with FinCEN urging FIs to remain vigilant against Russian efforts to evade US export controls.

Each new rule and regulation adds to an already complex compliance landscape that companies and FIs are expected to navigate. It is important for firms to not only understand how these new rules and compliance expectations impact their operations but to ensure that they have the resources to fully incorporate them into their compliance programmes and reevaluate areas of their business that may pose additional risk.

Enforcement

In addition to releasing compliance guidance and new rules and regulations, US government agencies have demonstrated their commitment to enforcement as a way to further incentivise corporate compliance.

Law enforcement and government agencies have been particularly active in the crypto space over the last year. In November, the Treasury, the DOJ and the Commodity Futures Trading Commission levied record-breaking penalties totalling over $4bn against one crypto exchange for US sanctions, anti-money laundering (AML) and derivatives exchange requirement violations. In a separate action, in April, the BIS and OFAC imposed a combined $3.3m in civil penalties on a large US technology company for apparent violations of US export controls and sanctions laws.

In January 2023, US law enforcement authorities in Miami arrested the founder and majority owner of a Hong Kong-based virtual currency exchange on charges of money laundering and violations of the Bank Secrecy Act. The following day,

FinCEN issued an order identifying the exchange as a "primary money laundering concern" under section 9714 of the Combatting Russian Money Laundering Act. The order was FinCEN's first under section 9714, which authorises the secretary of the treasury to identify non-US FIs, classes of transactions or types of accounts as primary money laundering concerns in connection with Russian illicit finance and impose "special measures" to combat such concerns without engaging in the notice and comment rulemaking process required by 311 actions.

The government continues to allocate additional resources to strengthen its enforcement posture. For example, the DOJ announced that it was adding more than 25 prosecutors to its NSD to focus on sanctions and export control violation and hired its first-ever chief counsel and deputy chief counsel for corporate enforcement. It also created the Disruptive Technology Task Force to target illegal transfers of sensitive technologies to Russia and other countries of concern, and added additional resources to the Bank Integrity Unit within the Money Laundering and Asset Recovery Section.

Perhaps the most notable feature of these recent enforcement actions has been the number of agencies involved, as well as an unprecedented level of coordination across agencies in investigating and bringing actions. Whether acting individually or together, multiple, well-resourced agencies are signalling a more aggressive posture when it comes to enforcing AML, export controls and sanctions violations.

How companies can respond

Companies should carefully implement and maintain their compliance programmes. This includes ensuring that controls, such as customer due diligence and transaction monitoring, are effectively calibrated to the risks present in a company's operating environment. These tools are often overlooked because they take time to build and are resource-intensive to effectively maintain. With the potential of multibillion-dollar enforcement actions, investing in these controls now can save companies money in the long run.

Even where a company has implemented a sophisticated compliance programme, it is important to regularly refresh risk assessments, particularly where the company has business touching on fast-evolving or otherwise high-risk areas such as digital assets, Russia and the Middle East, or involves high-tech products, such as AI, semiconductors and semiconductor manufacturing technology.

Beyond implementing programmes and assessing risks, companies should take steps to plan for and address deficiencies in their control environment. Depending on the circumstances, companies should be ready to file SARs, and in certain cases, organisations should carefully evaluate whether potential violations should be disclosed to relevant government authorities.

Government agencies are tightening the reins on corporate compliance and are showing an increasing appetite to enforce the growing suite of regulations in this arena. Companies are best positioned to weather the expanding scope of national security-related rules and regulations and increased enforcement if they have robust compliance programmes in place that enable them to respond quickly and effectively to new legal standards, red flags and threat actors, as well as knowing what actions to take when suspicious activity or potential violations are detected. ■

This article first appeared in the February 2024 issue of Financier Worldwide magazine. Permission to use this reprint has been granted by the publisher.