KILPATRICK TOWNSEND

4 KEY TAKEAWAYS

OFAC Enforcement Actions Thus Far in 2023

Although there were not any published sanctions enforcement actions during the first two months of 2023, since March, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has released information on nine enforcement actions with penalties totaling over $556 million. One of those includes an enforcement action against a U.S. company and a former company executive for his role in the alleged sanctions violations. The following are notable takeaways from the enforcement actions for the first half of 2023.

1

Companies with smaller, non-core business lines should exercise proper oversight to ensure sanctions compliance. A major U.S.-based Bank agreed to pay the Federal Reserve Board and OFAC a fine totaling $97.8 million for its inadequate oversight of a European Bank's compliance risks, which allegedly enabled the apparent violation of U.S. sanctions against Iran, Syria, and Sudan. Prior to its acquisition, the Bank's predecessor provided a relationship European Bank with two versions of a trade sourcing platform. One version (the Hosted version) enabled the European Bank to manage certain of its own trade finance instruments on behalf of its clients, while the other version permitted the predecessor bank to process the trade transactions on behalf of the European Bank. Under the Hosted version, the European Bank had primary responsibility for screening for OFAC sanctions issues related to the transactions. Following a request by the European Bank, a mid-level manager within the predecessor bank approved a customized version of the Hosted software for the European Bank to use on transactions involving OFAC-sanctioned jurisdictions and persons. OFAC noted that, for seven years, the U.S.-based Bank's senior management should have reasonably known that the European Bank was using the Hosted version of the software to engage in transactions with OFAC-sanctions jurisdictions and persons. For example, after acquiring the processor bank, personnel at the U.S.-based Bank raised on multiple occasions, including to senior management, the potential sanctions-related risks arising from the trade insourcing relationships it inherited from the predecessor Bank. OFAC also found that there was no regular or systematic process to periodically review the European Bank's use of the Hosted software to confirm that it was appropriately screening for OFAC compliance. The U.S. Bank voluntarily self-disclosed the violations.

Exporters should gather all information on customers to spot red flags and screen the fullest range of available data; foreign-based subsidiaries should be properly integrated into sanctions and export compliance programs to minimize risks; testing or auditing are important tools to ensure a compliance program is working as designed and weaknesses are promptly remediated. A U.S.-based software maker agreed to pay OFAC and the Department of Commerce's Bureau of Industry and Security a total of $3.3 million to settle apparent violations of sanctions and export control laws relating to OFAC's Cuba, Iran, Syria, and Ukraine-/Russia-related sanctions programs. The violations stem from the software maker's volume licensing sales and incentive programs through which two of its subsidiaries in Ireland and Russia used third-party distributors and resellers. After purchasing the software, an end customer would download or otherwise access a copy of the software, install it, and activate it using a product key. The process of facilitating the downloads, including license activations, relied, at least in part, on U.S.-based servers and systems managed by persons in the U.S. or third countries. OFAC found that, by operating through third-party distributors and resellers, the software maker was inadvertently providing prohibited software and services to blocked persons and/or end users in sanctioned jurisdictions. OFAC noted that the cause of the apparent violations included a lack of

2

2

prohibited software and services to blocked persons and/or end users in sanctioned jurisdictions. OFAC noted that the cause of the apparent violations included a lack of complete or accurate information on the identities of the product's end customers. OFAC found that, at times, employees of the Russian subsidiary appeared to have intentionally circumvented the company's screening tools to prevent other affiliates from knowing the identity of the ultimate end customers. OFAC also found that the software maker had, on numerous occasions, failed to timely screen and evaluate pre-existing customers following changes to the Specifically Designated Nationals and Blocked Persons (SDN) List and implement timely corrective measures to avoid continued dealings with SDNs or blocked persons. The software maker's screening did not identify blocked parties that, although not on the SDN List, were owned 50 percent or more by SDNs, and also did not include common variations of the restricted party names, which resulted in the software maker engaging in ongoing business relationships with SDNs or blocked persons. OFAC noted that periodic auditing is an important tool to ensure that company employees, including those in foreign jurisdictions, adhere to the company's compliance programs. The software maker voluntarily self-disclosed the violations.

3

Company management may face individual liability for violating U.S. sanctions when engaging in, approving, or directing prohibited transactions; conduct implicating OFAC sanctions should be authorized by OFAC (including by general or specific license) before a Company engages in the activity; pre- and post-acquisition due diligence is important in order to identify and promptly remediate compliance deficiencies. A U.S.-based skincare company agreed to pay close to $3.3 million to settle apparent violations of OFAC sanctions concerning Iran. A former executive of the Company agreed separately to pay $175,000 to settle their potential civil liability for three apparent violations of OFAC's Iran sanctions arising from their role as a manager. The executive, other Company executives, and the CEO of an Iran distributor entered into an exclusive agreement to sell the Company's products in the Middle East, including Iran. The executive signed the distribution agreement, and the Company began exporting its products to Iran through the distributor while the Company had a pending application with OFAC for a specific license. Years after the first distribution agreement, the executive signed a new distribution agreement with the Iranian distributor's CEO, this time for a related UAE-based company to become the Company's sole distributor in the Middle East. OFAC determined that the executive should have understood that the UAE Distributor would export the Company's products to Iran. OFAC found that despite the Company's knowledge that an OFAC license would be required to lawfully export certain products to Iran, the Company nonetheless completed shipments to Iran via the UAE Distributor, through departments generally overseen by the executive. The Company was eventually acquired by another entity. The acquiring entity did not learn of the Company's Iran-related business until 2 months after the acquisition deal closed. The acquiring entity's general counsel directed the executive to instruct the UAE Distributor to cease all exports of the Company's products to Iran. The executive followed the demand, but also alerted another senior Company executive of the need to ensure that the UAE Distributor's CEO would not suggest that any Company executive approved the exports of the Company's products to Iran. For an additional 2 ½ years, the executive and other senior Company executives continued working with the UEA Distributor to export the Company's products to Iran. The Company voluntarily self-disclosed the violations.

IP screening and geofencing are important compliance tools; financial institutions should not rely on unsubstantiated assurances and instead work to investigate red flags. A foreign bank agreed to pay $3.4 million to settle its potential civil liability for apparent violations of OFAC sanctions concerning Crimea. For a period of 2 years, a customer of the foreign bank used the bank's e-banking platform from an IP address in Crimea to send payments to recipients in Crimea through U.S. correspondent banks. In one instance, one U.S. correspondent bank rejected the customer's payments citing potential connection to Crimea and alerted the foreign bank. The foreign bank requested additional information from the customer, but the customer falsely assured the foreign bank that none of the transactions involved Crimea. Based on this information, the foreign bank re-routed the rejected payments to a different U.S.-correspondent bank, which ultimately processed the transaction. OFAC found that the foreign bank had reason to know that the customer's assurances were

4

Crimea. Based on this information, the foreign bank re-routed the rejected payments to a different U.S.-correspondent bank, which ultimately processed the transaction. OFAC found that the foreign bank had reason to know that the customer's assurances were incorrect because when it onboarded the customer, the foreign bank had obtained "Know Your Customer" data, including addresses, telephone numbers, and a customer questionnaire, indicating the customer's physical presence in Crimea. OFAC found that although the foreign bank collected customer IP data, it did not integrate the data into its sanctions screening process. OFAC found that the foreign bank violated sanctions by causing the exportation from the U.S. of financial services to Crimea. This appears to be the first enforcement action in which OFAC has highlighted "geofencing" as a tool for sanctions remediation.

4

For more information, please contact: Mauricio Escobar: mescobar@kilpatricktownsend.com

www.kilpatricktownsend.com

Related People



Mauricio Escobar
t 281.809.4364
mescobar@ktslaw.com