KILPATRICK TOWNSEND

4 KEY TAKEAWAYS

OFAC Enforcement Actions Thus Far in 2021

Compared to prior years, this first half of 2021 has seen a drop in the number of published enforcement actions by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). The reduction is likely attributed to the new U.S. administration's desire to realign and refocus its sanctions programs. The remainder of 2021, and perhaps through the current administration's term, is likely to see an increase in published enforcement actions. Notwithstanding, there are still some notable enforcement actions this year, including the first-ever resolution pursuant to the U.S. Department of Justice's (DOJ) Export Control and Sanctions Enforcement Policy for Business Organizations.

Kilpatrick Townsend's Mauricio Escobar provides the following notable takeaways.

1

Software companies should implement GeoIP blocking and ensure they fully integrate acquired companies into their export controls and sanctions compliance programs. SAP SE (SAP), software company headquartered in Germany, agreed to pay a combined $8M to settle violations of the Export Administration Regulations and the Iranian Transactions and Sanctions Regulations. The resolution involved the U.S. Departments of Justice, Treasury and Commerce. SAP, through its overseas business partners, had illegally exported its U.S.-made software products (including upgrades and/or software patches) to users located in Iran. Certain SAP senior executives were aware that geolocation filters that identify and block Iranian downloads were not being utilized by the company nor its U.S.-based content delivery provider, and the company did not remedy the issue for years. A vast majority of downloads went to 14 companies, with which SAP partners in Turkey, UAE, Germany and Malaysia. Allegedly, SAP knew the partners were Iranian-controlled front companies. The U.S. government also found that SAP's cloud business group companies (CBGs) permitted approximately 2,360 Iranian users to access U.S.-based cloud services from Iran. SAP became aware through pre-acquisition due diligence and post-acquisition export control-specific audits that the CBGs lacked adequate export control and sanctions compliance processes. SAP failed to integrate the CBGs into its more robust export controls and sanctions compliance program. SAP self-disclosed the apparent violations. This was the first-ever resolution pursuant to the DOJs Export Control and Sanctions Enforcement Policy for Business Organizations. As part of its settlement, SAP agreed to conduct internal audits of its compliance with U.S. export control laws and produce those reports to the Department of Commerce/Bureau of Industry and Security for a period of 3 years.

2

Failure to fully understand the parameters of federal programs can lead to sanctions violations. MoneyGram Payment Systems, Inc. (MoneyGram), headquartered in Texas, agreed to settle apparent violations of various sanctions programs arising out of its involvement in the DOJ's Federal Bureau of Prisons (BOP). MoneyGram provided money transfer services to the BOP, which allowed inmates to send and receive funds into and out of their personal commissary accounts. MoneyGram did not screen the inmates against OFAC's Specially Designated Nationals and Blocked Persons List (SDN List). MoneyGram knew that some of the inmates for whom it was processing transactions could be on the SDN List, but erroneously believed that such screening of inmates in federal prison was not expected under the BOP program. This enforcement action highlights the importance for all financial services providers to understand the sanctions risks associated with those services and maintain robust sanctions screening software and processes even when participating in federal programs.

3

Any U.S. financial system connection can trigger an enforcement action. PT Bukit Muria Jaya (BMJ), a paper products manufacturer located in Indonesia, agreed to settle apparent violations of the North Korea Sanctions Regulations resulting from its exports of cigarette paper to entities located in or doing business on behalf of the Democratic People's Republic of Korea (DPRK). BMJ also exported to an intermediary in China that procured the cigarette paper on behalf of an OFAC-designated North Korean entity. BMJ initially referenced DPRK entities on its transactional documents, but at the request of its customers, certain BMJ employees later replaced those references with the names of intermediaries located in third countries. BMJ directed payments for these exports to its U.S. dollar bank account at a non-U.S. bank, which caused U.S. banks to clear wire transfers related to the shipments. This enforcement action highlights the risks to non-U.S. persons who involve the U.S. financial systems in commercial activity with an OFAC-sanctioned country, region, or person.

4

Internal Controls such as IT solutions must be calibrated to address the company's risk profile. Payoneer Inc. (Payoneer), a New York-based online money transmitter, agreed to pay more than $1.4M to settle its apparent violations of multiple sanctions programs. Although Payoneer had policies and procedures in place that prohibited transactions involving parties in sanctioned locations, the testing and auditing of those internal controls failed to identify compliance deficiencies that led to the apparent violations. The control breakdowns included: (i) weak algorithms that allowed close matches to SDN List entries not to be flagged by its IT solution filter; (ii) failure to screen for Business Identifier Codes even when the SDN List entries contained them; (iii) during backlog periods, allowing flagged and pending payments to be automatically released without further review; (iv) lack of focus on sanctioned countries because the company was not monitoring IP addresses or flagging addresses in sanctioned countries.

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