OFAC Highlights the Importance of Integrating IP Address and KYC Data in Sanctions Compliance

By Hdeel Abdelhady | June 23, 2023

The recent settlement between the Office of Foreign Assets Control (OFAC) and Swedbank Latvia for apparent violations of Ukraine-/Russia-Related sanctions underscores the importance of integrating Internet Protocol (IP) address/geolocation and other data into sanctions compliance practices, especially for entities engaged in online banking and commerce. OFAC expects parties obligated to comply with U.S. sanctions programs to integrate relevant available information, such as KYC (know your customer) information in the case of financial institutions.

Apparent Violations of Ukraine-/Russia-Related Sanctions Involving E-Banking and Correspondent Banks

According to OFAC's June 20, 2023 Enforcement Release, Swedbank Latvia agreed to settle its potential civil liability for 386 transactions conducted through its e-banking platform between February 2015 and October 2016. These transactions involved accounts held by an individual customer in Crimea in the shipping industry, who owned three special purpose companies that each had an account with Swedbank Latvia. The accounts were established before the Ukraine-/Russia-Related sanctions were promulgated in 2014, following Russia's "annexation" of Crimea.[1]

The customer conducted the 2015 and 2016 electronic transactions from an IP address in Crimea and sent payments to persons in Crimea. These transactions were prohibited when conducted, under Executive Order 13685 of December 14, 2014. EO 13685 prohibits, among other activities: "the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, services, or technology to the Crimea region of Ukraine," and transactions that evade or avoid, or have the purpose of evading or avoiding the Executive Order's prohibitions, or cause a violation of its prohibitions.[2]

One U.S. correspondent bank rejected payments transactions initiated by the individual customer through Swedbank Latvia's e-banking platform, alerted Swedbank Latvia, and cited a potential connection to Crimea as the reason for the rejection. In response, Swedbank Latvia requested information from the customer, who "falsely assured" the bank "that none of the transactions involved Crimea." Based on this assurance, Swedbank Latvia rerouted the rejected transactions to another U.S. correspondent bank that processed them. The transactions violated EC 13685's prohibitions the provision to Crimea of services and evasive transactions.

[1] The Ukraine-/Russia-Related Sanctions program, at 31 C.F.R. Part 589, is separate from the Russian Harmful Activities Sanctions program at 31 C.F.R. Part 587. The latter responds to Russia's invasion of Ukraine in 2022.
[2] Exec. Order 13685 §§ 1(a)(iii), 6(a).

OFAC's Findings and Compliance Expectations

OFAC determined that Swedbank Latvia had reason to know that its customer was present in Crimea when the transactions were conducted through its e-banking platform, including because the bank had "collected and stored customer IP data." However, Swedbank Latvia did "not integrate this IP data into its sanctions screening processes." The same IP address data, had it been integrated, would have indicated that the customer was "present in Crimea at the time of the Apparent Violations."

OFAC also reasoned that Swedbank Latvia possessed KYC data, such as the customer's address and telephone number, "clearly indicating that" the customer and the three special purpose companies "had a physical presence in Crimea," and should have integrated that information for sanctions compliance purposes, particularly given its proximity to Crimea, a comprehensively sanctioned region.

The maximum assessable civil monetary penalty exceeded $112 million, but the apparent violations were settled for $3,430,900, taking into account various aggravating and mitigating factors outlined in OFAC's Enforcement Guidelines.[3] The mitigating factors included Swedbank's cooperation with OFAC, agreement to toll the statute of limitations,[4] offboarding of the individual customer and the three special purpose companies in 2016 and 2017, and implementation of remedial measures after discovering the violations through a lookback. These measures included the implementation of geofencing to prevent customers from sending online payments using IP addresses in comprehensively sanctioned jurisdictions.

It is worth noting that while Swedbank Latvia self-reported the apparent violations to OFAC, the disclosure did not qualify as a "voluntary self-disclosure" as defined by OFAC's Enforcement Guidelines. This may be due to the fact that the U.S. correspondent bank that rejected the transactions reported them to OFAC, as the U.S. correspondent bank would have been obligated to do under OFAC's recordkeeping and reporting regulations.[5] Notice by a violating party to OFAC of an apparent violation is not a "voluntary self-disclosure" if a third party obligated to block or reject the transaction notifies OFAC of the apparent violation.[6]

Key Takeaways

OFAC's enforcement releases are valuable sources of actionable compliance information. They are written in plain English, discuss operative facts, and convey (explicitly and implicitly) OFAC's compliance expectations and understanding of its regulations.

The key takeaways from this case are as follows.

- **Integrate Compliance-Relevant Data, Including KYC**. Financial institutions and other parties obligated to comply with U.S. sanctions regulations should integrate customer and other information collected for distinct regulatory compliance purpose, including anti-money laundering (AML) and sanctions compliance. As demonstrated by the Swedbank Latvia settlement, information obtained for AML compliance purposes, such as through KYC processes,

[3] Economic Sanctions Enforcement Guidelines, 31 C.F.R. Part 501, Appendix A ("**Enforcement Guidelines**").

[4] Note that a party's declination to toll the statute limitations is not an "aggravating factor" under the Enforcement Guidelines.

[5] *See* 31 C.F.R. § 501.604(c) (requiring rejected transactions to be reported to OFAC within ten business days).

[6] Enforcement Guidelines.

is relevant to sanctions compliance. OFAC emphasizes the importance of incorporating all relevant information – such as passport information, phone numbers, nationalities, and addresses – for effective, risk-based sanctions compliance.

- **Integrate IP Address/Geolocation Data**. Parties involved in electronic banking, payments, and commerce, among others, should integrate – commensurate with their risk – IP address/geolocation data into sanctions compliance programs related to comprehensively sanctioned or nearly comprehensively sanctioned countries and regions (Cuba, Iran, Russia, North Korea, Syria, and the Crimea, Donetsk, and Luhansk regions of Ukraine).[7] This data is commonly collected, stored, and used for various purposes, including advertising and security.[8] Additional measures may be necessary for parties engaged exclusively in online commerce. OFAC has stated that such parties should take additional steps to "know their customers directly," considering, for example, that IP information can be reassigned or masked.

By considering these key takeaways and generally implementing appropriate, risk-based measures, entities may enhance their sanctions compliance practices and mitigate the risk of potential violations.

***

The Swedbank Latvia settlement release is available here.

***

Hdeel Abdelhady, an attorney based in Washington, D.C., is Principal at MassPoint Legal and Strategy PLLC. To view more of her writings on sanctions, please see MassPoint's blog and publications.

***

[7] Of course, data collection and usage must also comply with other applicable law, including the privacy laws of one or more jurisdictions. Conflicts between substantive laws would need to be addressed and managed. Such issues are beyond the scope of this piece.

[8] *See* OFAC FAQ No. 73, Compliance for Internet, Web Based Activities and Personal Communications