Amazon's settlement with OFAC puts e-commerce companies on notice

July 8, 2020

Today the Office of Foreign Assets Control (OFAC) announced a settlement agreement with Amazon for apparent violations of U.S. sanctions regulations by the company. The announcement puts e-commerce and online companies on notice to increase their vigilance when it comes to sanctions screening.

According to OFAC, Amazon violated U.S. regulations by conducting retail e-commerce transactions with persons in sanctioned territories, persons on OFAC's List of Specially Designated Nationals (SDNs), and sanctioned country embassies around the world. OFAC found particular fault with Amazon's sanctions screening program, which failed to take into consideration all of the transaction and consumer information that was relevant to sanctions compliance. For example, OFAC noted that Amazon's system failed to stop transactions that included the names of sanctioned territories and consumers with exact name matches to parties on the SDN List. OFAC noted that Amazon also failed to halt transactions involving common alternative spellings of sanctioned locations ("Krimea" instead of "Crimea") or known cities in sanctioned locations ("Yalta," which is in the Crimea region).

The announcement reads like a roadmap for what e-commerce and online companies should be doing to ensure compliance with OFAC's regulations. Among other measures, companies should consider:

- **Tailored controls**: E-commerce companies should adopt screening programs that are adapted to the fast-paced and often high volume world of e-commerce. By their nature, e-commerce companies must rely on highly automated systems to screen transactions for sanctions compliance. The key is to design those programs to capture risky transactions without generating an overwhelming number of "false positives" that require individualized review by human analysts.
- **Poor data**: Companies should take into consideration the limited or poor quality data that is often inherent in online transactions, data that can easily include misspelled or alternatively spelled locations. Companies handling online transactions, especially those without a stable customer base, need to be able to efficiently screen and hold transactions that raise sanctions compliance concerns, despite these challenges. Some companies may also benefit from improving the quality of data collected from customers, which will make screening more reliable and reduce false positives over time.
- **The right data**: E-commerce companies must consider all of the data that they collect on customers and transactions and determine which elements contain information relevant to sanctions screening. That data may exist in different databases or parts of companies' systems and may need to be stitched together to obtain a full view of potential sanctions risks.

- **IP blocking**: Companies should review their Internet Protocol (IP) blocking controls, which deny access from IP addresses associated with sanctioned territories, to ensure that they are effective. While OFAC recognized improvements to Amazon's IP blocking controls in its announcement, e-commerce companies should be wary of overreliance on IP blocking, which can miss customers that access sites through Virtual Private Networks (VPNs) or other tools that anonymize customers' locations.
- **Testing**: Testing is the only way to tell if a sanctions compliance program is working as intended. E-commerce companies should dig into their customer and transaction data, with help from qualified sanctions data analysts and counsel as needed, to periodically review whether their sanctions compliance screening program is capturing the right transactions and dispositioning them appropriately.
- **Training**: OFAC recognized that Amazon took remedial action to ensure that employees received training tailored to their job responsibilities. This type of targeted process-based training, in addition to broader "awareness" training, is the most effective way to ensure that employees understand their responsibilities and know where to get help on sanctions issues.

E-commerce and technology companies are often lucky to have deep benches of data science and programming expertise that can be used to design targeted, risk-based compliance solutions. But technology companies also tend to capture a lot of relevant data on users that must be considered when adopting sanctions compliance solutions. Getting a handle on what data is collected, and how to analyze it in light of OFAC's rules is the first step to ensuring compliance – and avoiding penalties and bad press.