NOW & NEXT

Export Controls Alert

APRIL 13, 2023

Microsoft settles OFAC and BIS sanctions violations for $3.3M

By Christopher D. Grigg and Alexandra López-Casero

Alleged export control and sanctions violations relating to software exports to sanctioned jurisdictions could have cost Microsoft over $400M—here's how your company can reduce risk.

What's the Impact?

- All exporters, including technology companies, must be vigilant about screening end users and weeding out blocked persons and entities.
- Exporters should gather all customer and business partner identifiers to spot red flags and screen the fullest range of available data.
- Foreign-based subsidiaries, partners, and sales teams can generate risk if not properly integrated into meaningful sanctions and export compliance programs.
- Like sanctions and export control laws, effective compliance programs are not static; companies should regularly audit their practices to identify opportunities for improvement.

On April 6, the Department of the Treasury published an Enforcement Release detailing Microsoft Corporation's settlement with the Treasury's Office of Foreign Assets Control ("OFAC")

for $2,980,265.86, relating to alleged violations of OFAC's Cuba, Iran, Syria, and Ukraine-/Russia-related sanctions programs. This settlement was part of a coordinated enforcement action with the Department of Commerce's Bureau of Industry and Security ("BIS") and resulted in a combined $3.3 million in civil penalties against Microsoft for alleged and apparent violations of U.S. export controls and sanctions laws.

According to the Enforcement Release, Microsoft engaged in over 1,000 alleged violations of OFAC sanctions programs by selling software licenses and providing related services to end users that included persons listed on OFAC's Specially Designated Nationals and Blocked Persons List (the "SDN List") and blocked persons located in Cuba, Iran, Syria, Russia, and the Crimea region of Ukraine. Microsoft voluntarily self-disclosed the alleged violations to both BIS and OFAC, cooperated with the joint investigation conducted by BIS's Office of Export Enforcement and OFAC, and took remedial measures after discovering the conduct at issue, which predated the export controls and sanctions imposed in connection with the current Russian war in Ukraine.

How did the violations happen?

Sanctions and export controls are complex, and compliance can be extremely challenging, especially for companies active in international supply and distribution markets. The Enforcement Release highlights that even the largest companies with robust compliance programs can err, especially if they do not actively monitor their foreign affiliates' activities. Here, the violations appear to have occurred in the context of Microsoft's volume licensing sales and incentive programs through which two Microsoft subsidiaries in Ireland and Russia utilized third-party distributors and resellers to sell Microsoft software products and also relied on an indirect resale model through third-party licensing solution partners.

This sales model apparently allowed end users to access a copy of the software, install the software on its devices, and activate and manage the software using a product key, relying at least in part on U.S.-based servers.

According to OFAC, this also meant that end customers that were blocked via the Ukraine sanctions program benefitted from certain services processed, at least in part, through these U.S.-based servers. By operating through these third-party distributors and/or supporting sales or services benefiting the prohibited parties, Microsoft was inadvertently providing prohibited software and services to SDNs, blocked persons, and/or end users in sanctioned jurisdictions. The software and services in question were not eligible for any general licenses or other exemptions. The Enforcement Release not only details the sales and service models that apparently enabled the violations to occur but also details alleged screening gaps, including failure to screen existing customers after changes were made to OFAC's SDN List and failure to identify Russiaa and China-based parties and entities.

OFAC's enforcement notice observed that the cause of the apparent violations "included the lack of complete or accurate information on the identities of the end customers for Microsoft's products." OFAC also noted additional shortcomings in restricted-party screening. For example,

OFAC indicated that, in some instances, when Microsoft Ireland was made aware of the end customer by the distributor or reseller, "Microsoft's restricted-party screening architecture did not aggregate information known to Microsoft, such as an address, name, and tax-identification number, across its databases to identify SDNs or blocked persons."

OFAC's reference to tax ID numbers is noteworthy because, thus far, OFAC has not stressed that tax ID numbers should also be screened. Many, if not most, commercially available screening tools do not offer the option to screen parties through their tax ID. On the other hand, experienced exporters know that OFAC's online sanctions list search tool, which is available for so-called "manual" searches, offers a generic identification number search field. The key takeaway here is not to abandon commercial screening software but rather that companies should gather all customer and other party identifiers so that they can spot red flags and screen the fullest range of available data.

In a number of cases Microsoft apparently also failed to timely screen and evaluate pre-existing customers following changes to the SDN List and implement timely corrective measures to avoid continued dealings with SDNs or blocked persons. Further, according to OFAC, "Microsoft's screening against restricted-party lists did not identify blocked parties not specifically listed on the SDN List, but owned 50 percent or more by SDNs, or SDNs' Cyrillic or Chinese names, even though many customers in Russia and China supplied order and customer information in their native scripts. These failures, which also included missing common variations of the restricted party names, resulted in Microsoft engaging in ongoing business relationships with SDNs or blocked persons." It would have been helpful if OFAC had clarified if the parties with sanctioned ownership above 50% where in or outside Russia. Further, just as with tax ID screening, many screening tools do not offer screening in Cyrillic or Chinese. Moreover, this is not a realistic screening option for companies that screen transactions through compliance staff located outside China (and certainly outside Russia), who in most cases do not have the language skills and technical tools to (correctly) input names in Chinese or Cyrillic.

The OFAC settlement

Microsoft agreed to pay $2,980,265.86 to settle its potential civil liability stemming from the exportation of its software and services in apparent violation of the Cuban Assets Control Regulations, the Iranian Transactions and Sanctions Regulations, the Syrian Sanctions Regulations, and the Ukraine-/Russia-Related Sanctions Regulations.

While the statutory max could have resulted in $404,646,121.89 in civil monetary penalties, the final amount reflects OFAC's conclusion that (a) the conduct was non-egregious, (b) Microsoft voluntarily self-disclosed, and (c) Microsoft took "significant remedial measures" upon discovery of the violations. These factors are typical of the considerations that the three primary federal sanctions and export enforcement agencies—OFAC, BIS, and the U.S. Department of Justice—weigh when evaluating corporate wrongdoing.

The BIS settlement

According to BIS, on seven occasions prior to the Ukraine war, employees of Microsoft Russia caused another Microsoft subsidiary to enter into or sell software licensing agreements that would allow the transfer or access to software subject to the Export Administration Regulations by FAU 'Glavgosekspertiza Rossii' and United Shipbuilding Corporation Joint Stock Company ("United Shipbuilding Corporation"), both of which were on BIS's Entity List. The alleged time frame was between December 28, 2016, and December 22, 2017. FAU 'Glavgosekspertiza Rossii' is a Russian federal institution involved with construction projects, including the Kerch Bridge, which was built to connect Crimea to Russia after its 2014 invasion. United Shipbuilding Corporation is responsible for developing and building the Russian Navy's warships. In the case of FAU 'Glavgosekspertiza Rossii,' BIS alleged that certain Russia-based employees of Microsoft Russia ordered software licenses through one of Microsoft's open sales programs in the names of parties not on the Entity List; in the case of United Shipbuilding, an increased number of software licenses were added under non-listed affiliates' enterprise agreements.

Lessons learned

This settlement reflects U.S. government agencies' stringent commitment to preventing foreign adversaries and bad actors from obtaining and benefitting from U.S. technologies and demonstrates that even inadvertent engagement with blocked persons and entities will not be tolerated.

Businesses in advanced technology fields should take heed and learn lessons from this recent action. Here are some key steps your company can take to protect its assets, products, and reputation:

Improve your screening processes

According to OFAC, Microsoft's restricted-party screening underperformed in many instances by failing to identify:

- SDNs or blocked persons
- Blocked parties not explicitly named on the SDN List but owned 50 percent or more by SDNs
- SDNs' Cyrillic or Chinese names

OFAC concluded that "a world-leading technology company operating globally with substantial experience and expertise in software and related services sales and transactions" should not have tolerated these screening malfunctions. Microsoft's leading status in the tech space was deemed to be an aggravating factor.

This Enforcement Release reiterates OFAC's view from other cases where large, globally operating companies are held to a higher standard than others. This case also highlights the common sanctions risks of offering software and related services through IT platforms. Engage talent to review and assess potential blind spots in your screening processes.

Stay on top of SDN and Entity List changes

OFAC found a number of cases in which Microsoft failed to timely screen and evaluate existing customers following changes to the SDN List and also failed to implement timely corrective measures to prevent further dealings with SDNs or blocked persons.

The SDN list and BIS's Entity List and Unverified List are not stagnant documents, and companies must stay on top of changes to the list to minimize their exposure. Proactive screening, review, and preventive actions can minimize the risk that your company will inadvertently engage with blocked parties.

Keep your customers close

OFAC acknowledges that even vigilant companies can fall prey to evasion tactics by bad actors. The Enforcement Release reiterated that:

> Sanctioned Russian enterprises may use a variety of means, including obscuring the identity of actual end users, to circumvent U.S. restrictions. All persons continuing to engage in business with Russia should be aware of such evasion techniques and associated red flags, such as those described in the Treasury–Commerce–Justice March 2023 Alert, "Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls" and FinCEN's March 2022 Alert, "FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts."

In announcing the settlement, both BIS and OFAC made clear that they would seek to hold U.S. companies accountable for the activities of their foreign subsidiaries, distributors, and resellers. No matter how large or small your company is, foreign-based subsidiaries, distributors, and sales representatives can generate risk if not properly integrated into your company's compliance program. It is your responsibility to ensure your foreign affiliates and sales teams focus on screening, licensing, record-keeping, and the other hallmarks of effective sanctions and export compliance practices under U.S. law. According to the BIS Order and the OFAC notice resolving their respective enforcement actions, employees of Microsoft's foreign subsidiary discussed and devised techniques to circumvent screening controls through sales to affiliates of the listed entities. Companies should consider regularly auditing foreign-based sales activities and related communications and act swiftly to address any deficiencies or non-compliant behavior.

Compliance and cooperation are sound strategies

Microsoft's liability was reduced substantially from the statutory maximum due, in part, to Microsoft's voluntary self-disclosure and subsequent cooperation with the Treasury entities.

While self-reporting violations and cooperating with the government can reduce your risk of severe penalties, determining whether and when to voluntarily disclose suspected violations can be one of the most difficult and complex decisions a company can face. Companies weighing

whether to self-disclose should work closely with experienced counsel to avoid the many pitfalls that can arise.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Alexandra López-Casero
202.213.0171
alopezcasero@nixonpeabody.com

Christopher D. Grigg
213.629.6134
cgrigg@nixonpeabody.com