DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Enforcement Release: April 6, 2023

OFAC Settles with Microsoft Corporation for $2,980,265.86 Related to Apparent Violations of Multiple OFAC Sanctions Programs

Microsoft Corporation ("Microsoft") is a multinational technology company headquartered in Redmond, Washington. On behalf of itself, and its subsidiaries Microsoft Ireland Operations Ltd. ("Microsoft Ireland") and Microsoft Rus LLC ("Microsoft Russia") (collectively, the "Microsoft Entities"), Microsoft has agreed to pay $2,980,265.86 to settle its potential civil liability relating to the exportation of services or software from the United States to comprehensively sanctioned jurisdictions and to Specially Designated Nationals ("SDNs") or blocked persons in violation of OFAC's Cuba, Iran, Syria, and Ukraine-/Russia-Related sanctions programs. The majority of the apparent violations involved blocked Russian entities or persons located in the Crimea region of Ukraine, and occurred as a result of the Microsoft Entities' failure to identify and prevent the use of its products by prohibited parties. The settlement amount reflects OFAC's determination that the conduct of the Microsoft Entities was non-egregious and voluntarily self-disclosed, and further reflects the significant remedial measures Microsoft undertook upon discovery of the apparent violations.

This action was part of a joint administrative enforcement effort with the Bureau of Industry and Security (BIS), U.S. Department of Commerce, which settled with Microsoft for $624,013 for related violations of the Export Administration Regulations. In light of OFAC's settlement, BIS credited Microsoft $276,382 against its settlement figure, contingent upon Microsoft fulfilling its commitments under its settlement agreement with OFAC. Additional details surrounding the BIS action can be found at https://www.bis.doc.gov/index.php/enforcement.

Description of the OFAC Apparent Violations

Between July 2012 and April 2019, the Microsoft Entities engaged in 1,339 apparent violations of multiple OFAC sanctions programs when they sold software licenses, activated software licenses, and/or provided related services from servers and systems located in the United States and Ireland to SDNs, blocked persons, and other end users located in Cuba, Iran, Syria, Russia, and the Crimea region of Ukraine. The total value of these sales and related services was $12,105,189.79.

The apparent violations occurred in the context of Microsoft's volume licensing sales and incentive programs, under which the Microsoft Entities engaged with third-party distributors and resellers to sell Microsoft software products. In Russia, among other sales programs, the Microsoft Entities employed an indirect resale model through third-party Licensing Solution Partners ("LSPs"). Under this model, Microsoft Russia worked with LSPs to develop sales leads and negotiate bulk sales agreements with end customers, while the LSP and the end customer would negotiate the final sales price and sign a commercial supply agreement. Microsoft Ireland would bill the LSPs annually for licenses it supplied, and the LSPs would separately bill and collect payment from end customers.

Upon purchasing the software under this or a similar sales model, an end customer would download or otherwise access a copy of the software, install the software on its devices or networks, and activate the software using a product key. The end customer could then access, activate, and manage its software (e.g., for renewals, updates, and enhancements). The process of facilitating Microsoft software downloads, license activations, product key verifications, and subsequent usages relied, at least in part, on U.S.-based servers and systems managed by personnel in the United States or third countries. Similarly, end customers that were blocked pursuant to the Ukraine sanctions program benefitted from certain services processed, at least in part, through Microsoft's U.S.-based servers and systems.

Accordingly, when the Microsoft Entities, operating through third-party distributors and resellers, supported sales or arranged for services benefiting prohibited parties, the Microsoft Entities provided prohibited software and services to SDNs, blocked persons, and/or end customers in sanctioned jurisdictions. The software and related services at issue in the apparent violations were ineligible for any general licenses or other exemptions.

The causes of these apparent violations included the lack of complete or accurate information on the identities of the end customers for Microsoft's products. For example, in certain volume-licensing programs involving sales by intermediaries, Microsoft was not provided, nor did it otherwise obtain, complete or accurate information on the ultimate end customers for its products from Microsoft's distributors and resellers. At times, Microsoft Russia employees appear even to have intentionally circumvented Microsoft's screening controls to prevent other Microsoft affiliates from knowing the identity of the ultimate end customers. For example, following OFAC's 2014 designation of Stroygazmontazh, a Russian company operating in the oil and gas industry, and Microsoft's initial rejection of one of this entity's subsidiaries as a potential customer upon screening, certain Microsoft Russia employees successfully used a pseudonym for that subsidiary to arrange orders on behalf of the SDN.

In addition, during the time period in which the apparent violations occurred, there were shortcomings in Microsoft's restricted-party screening. In some instances, for example, 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. In a number of cases Microsoft also failed to timely screen and evaluate pre-existing customers following changes to OFAC's Specially Designated Nationals and Blocked Persons List ("SDN List") and implement timely corrective measures to avoid continued dealings with SDNs or blocked persons.

Further, 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.

In total, the Microsoft Entities appear to have engaged in 54 apparent violations of § 515.201(b)(2) of the Cuban Assets Control Regulations, 31 C.F.R. part 515 ("CACR"); 30 apparent violations of § 560.204 and § 560.206(a)(2) of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. part 560 ("ITSR"); 3 apparent violations of § 542.207 of the Syrian Sanctions Regulations, 31 C.F.R. part 542 ("SySR"); and 1,252 apparent violations of § 589.207 of the Ukraine-/Russia Related Sanctions Regulations, 31 C.F.R. part 589 ("URSR") (the "Apparent Violations").

Penalty Calculations and General Factors Analysis

The statutory maximum civil monetary penalty applicable in this matter is $404,646,121.89. OFAC determined that Microsoft voluntarily self-disclosed the Apparent Violations, and that the Apparent Violations constitute a non-egregious case. Accordingly, under OFAC's Economic Sanctions Enforcement Guidelines ("Enforcement Guidelines"), 31 C.F.R. part 501, app. A, the base civil monetary penalty amount applicable in this matter is $5,960,531.72, equaling one-half the transactional value for each of the Apparent Violations. The settlement amount of $2,980,265.86 reflects OFAC's consideration of the General Factors under the Enforcement Guidelines.

OFAC determined the following to be **aggravating factors**:

(1) The Microsoft Entities demonstrated a reckless disregard for U.S. sanctions by failing to identify that over a seven-year period, more than $12,000,000 worth of software and services were exported from the United States through Microsoft systems and servers to SDNs, blocked persons, and to multiple sanctioned jurisdictions. The Apparent Violations were not isolated or atypical in nature, and the Microsoft Entities had reason to know that such conduct was occurring.

(2) The Microsoft Entities harmed U.S. foreign policy objectives by providing U.S. software and related services that facilitated the operations of, or otherwise benefited, more than 100 SDNs or blocked persons, including major Russian enterprises that generated substantial revenues for the Russian state.

(3) Microsoft is a world-leading technology company operating globally with substantial experience and expertise in software and related services sales and transactions.

OFAC determined the following to be **mitigating factors**:

(1) Evidence in the record did not show that persons in Microsoft's U.S. offices or management were aware of the apparently violative activity at the time. Microsoft's Apparent Violations came to light in the course of a self-initiated lookback, after which it conducted a comprehensive investigation to discover the causes and extent of the conduct leading to the Apparent Violations. Among other efforts, Microsoft conducted a retrospective review of thousands of past transactions, engaged in extensive ownership research and data analysis, engaged a team of more than 20 Russian-speaking attorneys to analyze relevant correspondence, and conducted numerous interviews.

(2) Microsoft voluntarily self-disclosed the Apparent Violations to OFAC and cooperated with OFAC's investigation, including by proactively providing voluminous, detailed information and engaging responsively with OFAC.

(3) Microsoft terminated the accounts of the SDNs or blocked persons at issue, and deactivated the license keys so that the prohibited parties cannot activate Microsoft's software programs. Further, Microsoft updated its "suspension and shutdown" procedures to disable access to its products and services when a sanctioned party is discovered.

(4) Upon discovering the Apparent Violations, Microsoft undertook significant remedial measures and enhanced its sanctions compliance program through substantial investment and structural changes, including:

- Enhancing Microsoft's trade compliance program, which originally was developed based on a risk assessment undertaken before OFAC published *A Framework for OFAC Compliance Commitments* in May 2019.

- Improving the governance structure of Microsoft's sanctions compliance program and increasing its resources, including implementing enhancements to its screening resources, technology, and methodology.

- Prior to its suspension of new sales in Russia in March 2022, requiring that Russian service contracts be cleared by Microsoft's High Risk Deal Desk, a function that provides additional compliance oversight. The process further required pre-contract review of various risk factors, including a detailed review of the ultimate end customer, assessment of the deal structure to identify the beneficiary of Microsoft's services, and an internal analysis of any existing trade or sanctions restrictions. Microsoft had also reduced its reseller universe in Russia and undertook extensive vetting to select eligible participants.

- Implementing an "end-to-end" screening system that gathers data when an outside party makes its first contact with the company; collects risk-based, compliance-oriented data to enable accurate and reliable restricted-party screening; and screens its data on a persistent, rather than a transactional, basis.

- Improving the methods by which it researches potential sanctions matches, modifying the procedures to respond to matches, and expanding the scope and volume of data screened. For example, Microsoft deployed a multi-disciplinary internal investigative team to aid its contractors and full-time employees in reviewing and researching potential restricted-party hits. Collectively, the investigative team members are fluent or proficient in 16 foreign languages including Russian, Chinese, Farsi, and Arabic. The team researches corporate organizational documents, physical and email addresses, and various other open-source materials to identify SDNs or blocked persons, and has shared its findings with a provider of

commercial restricted-party screening lists, helping to enhance the utility of those lists for other subscribers.

- Deploying detailed sanctions compliance training for certain employees and jurisdictions, which is designed to take account of specific vulnerabilities identified throughout this disclosure process.

- Adopting a new "Three Lines of Defense" model to govern its trade compliance program, which emphasizes management oversight and compliance monitoring. Under the first line of defense, Microsoft personnel responsible for sales transactions are tasked with day-to-day responsibility for ensuring compliance, with support from Microsoft's trade and legal functions. The second line of defense consists of oversight of the first line by Microsoft's legal compliance, high-risk, financial integrity, and tax and trade units, which respond to questions or escalated issues as they arise and conduct quarterly testing. These compliance personnel are independent of the sales and marketing functions whose compliance they oversee, and report directly to Microsoft's senior management. The third line of defense consists of Microsoft's internal audit team, which performs regular independent audits and reports to Microsoft's leadership and board of directors.

- Terminating or otherwise disciplining the Microsoft Russia employees engaged in the activity described above.

Compliance Considerations

The increased use of internet-based computing and global demand for software applications has expanded the potential user base of technology, software, or services exported from the United States. Companies with sophisticated technology operations and a global customer base should ensure that their sanctions compliance controls remain commensurate with that risk and leverage appropriate technological compliance solutions. Such companies should also consider conducting a holistic risk assessment to identify and remediate instances where the company may, directly or indirectly, engage with OFAC-prohibited persons, parties, countries, or regions. Such an assessment is particularly important for companies operating in or exposed to high-risk jurisdictions.

This action also highlights the importance of companies conducting business through foreign-based subsidiaries, distributors, and resellers having sufficient visibility into end users with which they may have an ongoing relationship, including through the provision of services after an initial sale, to avoid engaging in business dealings with prohibited parties. Relatedly, because OFAC's SDN List is dynamic, when changes to OFAC's SDN List are implemented, companies should evaluate their pre-existing trade relationships to avoid dealings with prohibited parties.

This action further emphasizes the importance of ensuring a company's employees, including employees located in foreign jurisdictions, adhere to the company's sanctions compliance program. By engaging in periodic auditing, a company may promptly identify instances where employees have attempted to circumvent internal policies and procedures. Testing or auditing, whether

conducted on a specific element of a compliance program or at the enterprise-wide level, are important tools to ensure the program is working as designed and weaknesses are promptly remediated.

Lastly, this action underscores the persistent efforts of actors in the Russian Federation to evade U.S. sanctions. 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."

OFAC Enforcement and Compliance Resources

On May 2, 2019, OFAC published A Framework for OFAC Compliance Commitments in order to provide organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States or U.S. persons, or that use goods or services exported from the United States, with OFAC's perspective on the essential components of a sanctions compliance program. The *Framework* also outlines how OFAC may incorporate these components into its evaluation of apparent violations and resolution of investigations resulting in settlements. The *Framework* includes an appendix that offers a brief analysis of some of the root causes of apparent violations of U.S. economic and trade sanctions programs OFAC has identified during its investigative process.

Information concerning the civil penalties process can be found in the OFAC regulations governing each sanctions program; the Reporting, Procedures, and Penalties Regulations, 31 C.F.R. part 501; and the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, app. A. These references, as well as recent civil penalties and enforcement information, can be found on OFAC's website at: https://ofac.treasury.gov/civil-penalties-and-enforcement-information.

For more information regarding OFAC regulations, please go to: https://ofac.treasury.gov/sanctions-programs-and-country-information.