



**DEPARTMENT OF THE TREASURY
OFFICE OF FOREIGN ASSETS CONTROL**



Enforcement Release: October 27, 2026

**Extreme Networks Settles with OFAC for \$1,529,685 for
Apparent Violations of the Ukraine-/Russia-Related Sanctions Regulations**

Extreme Networks, Inc. (“Extreme”), a North Carolina-based artificial intelligence and cloud networking solutions provider, has agreed to pay \$1,529,685 to settle its potential civil liability for nine apparent violations arising from its dealings with a blocked Russian entity. Between September 2018 and March 2022, Extreme exported networking equipment and related services from the United States to an entity majority owned by a designated Russian state-owned company that manufactures air defense systems, missiles, and other war materiel. The settlement amount reflects OFAC’s determination that Extreme’s apparent violations were egregious and voluntarily self-disclosed.

Today’s action emphasizes the importance of sanctions-related diligence before acquiring a company or its assets; remaining vigilant regarding sanctions risks thereafter; and ensuring adequate oversight of foreign activities and operations. OFAC coordinated this action with the Department of Justice (DOJ), which today [announced resolution](#) of its parallel investigation.

Description of the Apparent Violations

Extreme and its affiliates operate globally, employing over 2,800 people across 29 countries. Around 2009, Extreme established a Russian subsidiary, Extreme Networks Rus LLC (“Extreme Russia”), which sold Extreme-branded networking products and services in Russia and provided post-sale customer support in Russia. Extreme Russia ceased operations in March 2022.

In March 2018, Extreme Russia purchased customer accounts and contracts to provide telecommunications equipment and services from a Russian networking business that specialized in business communications. Among the end users named in the contracts Extreme Russia acquired through the purchase agreement was Joint Stock Company (JSC) Moskovskiy Mashinostroitel'ny Zavod Avangard (MMZA), a Russian defense manufacturer majority owned by Russian state-owned defense company JSC Concern Almaz Antey (“Almaz Antey”). Almaz-Antey was designated on July 16, 2014 pursuant to Executive Order (“E.O.”) 13661.¹ Consequently, at all relevant times MMZA was a blocked person with which U.S. persons were prohibited from dealing, directly or indirectly.² MMZA was independently designated on June 28, 2022 pursuant to E.O. 14024 for operating in the defense and related material sector of the Russian economy, and specifically for producing missiles for Russia’s S-300 and S-400 anti-aircraft systems.

Extreme’s U.S.-led compliance team reviewed Extreme Russia’s March 2018 purchase agreement, which included the contract that named MMZA as the end-user. However, Extreme did not conduct

¹ See U.S. Department of the Treasury, [“Announcement of Treasury Sanctions on Entities Within the Financial Services and Energy Sectors of Russia, Against Arms or Related Materiel Entities, and those Undermining Ukraine’s Sovereignty”](#) (July 16, 2014).

² See 31 C.F.R. § 589.411; see also U.S. Department of the Treasury, [“Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property are Blocked”](#) (August 13, 2014).

sufficient due diligence to recognize that MMZA was blocked. Neither did Extreme raise questions concerning earlier purchases made under this contract that at times identified another Russian company, Dmitrovskiy Experimental Mechanical Plant (DEMZ), as the end-user.

Between September 2018 and September 2021, Extreme Russia maintained the relationship with MMZA, including through the negotiation and receipt of nine additional purchase orders (POs) for hardware (e.g., routing switches, ports, and power supplies) and software. During this period, Extreme Russia dealt directly with MMZA staff to develop these orders, including through in person meetings at MMZA's offices in Moscow and elsewhere, and by communicating through MMZA email addresses. Extreme Russia also provided training and post-sales support to MMZA staff on multiple occasions.

Extreme's U.S.-led centralized compliance function conducted sanctions and export controls screening for each of the nine POs under a company-wide policy to review all dealings involving Russia. Extreme, however, did not detect that it was dealing indirectly with a blocked entity, either ignoring or failing to appropriately respond to numerous indications that DEMZ was not in fact the true end user, and that instead Extreme was providing goods and services to MMZA. These red flags appeared in the POs themselves, seven of which included MMZA email addresses or identified MMZA's office address in Moscow as the ultimate destination for the purchased items even though DEMZ was named as the end user.

Additionally, in May 2018 and again in February 2019, Extreme's Regional Director for Northern and Eastern Europe, who supervised Extreme Russia staff, received two routine activity reports that included descriptions of Extreme Russia's dealings with MMZA. Further, on October 20, 2020 and again on November 10, 2020, during due diligence reviews for two of the POs, Extreme asked its third-party distributor to provide the relevant end-user's website. Despite DEMZ being identified as the end-user in the PO, the third-party distributor responded twice with MMZA's website. After Extreme expressed concerns about MMZA's apparent military affiliations, the third-party distributor deflected by providing DEMZ's website, claiming its earlier references to MMZA website were a mistake. Extreme ultimately decided to approve the POs without further investigation based on an end-user statement provided by the third-party distributor identifying DEMZ as the end-user.

Extreme also failed to stop MMZA personnel from registering for its proprietary online portal, which enabled customers to track contracts, submit support cases, and engage with technical tools. Extreme Russia personnel in fact instructed MMZA personnel to list DEMZ as their company name when registering for portal access, while they still used their MMZA email addresses. Although the portal registrations were also initially held up by the blanket policy to review dealings involving Russia, Extreme ultimately approved the registration requests, including in one instance after one of the MMZA employees failed to respond to a due diligence request asking for their company's name, address, and corporate email.

Ultimately, between September 2018 and March 2022, Extreme dealt in property in which a blocked person held an interest on nine occasions when it exported hardware and software from the United States to MMZA, in apparent violation of § 589.201 of the Ukraine-/Russia-Related Sanctions Regulations, 31 C.F.R. part 589 (the "Apparent Violations").

Penalty Calculations and General Factors Analysis

OFAC determined that Extreme voluntarily self-disclosed the Apparent Violations and that the Apparent Violations constitute an egregious case. Accordingly, under OFAC's Economic Sanctions Enforcement Guidelines (the "Enforcement Guidelines"), 31 C.F.R. part 501, app. A., the base civil monetary penalty applicable in this matter equals one-half of the statutory maximum, which is \$1,699,650.

The settlement amount of \$1,529,685 reflects OFAC's consideration of the General Factors under the Enforcement Guidelines. Extreme's obligation to pay a portion of the settlement amount will be deemed satisfied up to an equal amount of its payment of a fine to DOJ arising out of the same conduct. OFAC's Settlement Agreement with Extreme can be found [here](#).

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

- (1) Extreme acted with reckless disregard for U.S. sanctions when it failed to conduct sufficient due diligence to recognize that MMZA was a blocked person, and when it failed to heed numerous warning signs that MMZA was the ultimate recipient of the goods in the nine POs that Extreme ostensibly fulfilled for DEMZ.
- (2) Extreme had actual knowledge that it fulfilled the nine POs and had reason to know that MMZA was the actual end-user.
- (3) Extreme substantially harmed U.S. foreign policy objectives to deny the Russian Federation's ability to supply the military sectors of its economy and to degrade Russia's capacity to wage war against Ukraine by providing economic benefit to MMZA, a blocked Russian defense firm that describes itself as the sole supplier of Russia's S-300 and S-400 mobile surface-to-air missile systems.

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

- (1) Extreme has not been the subject of any OFAC enforcement action in the five years preceding the earliest date of the transactions giving rise to the Apparent Violations.
- (2) Extreme took substantial remedial actions to address the root cause of the Apparent Violations, including enhancing screening processes to better identify entities majority owned by a sanctioned party or with military or government affiliations; expanding end-user diligence procedures; hiring additional sanctions compliance personnel; increasing training for employees in compliance and customer-facing roles; and updating due diligence processes for mergers and acquisitions to include comprehensive screening of the target entity and its customers.

Compliance Considerations

This case highlights the importance of treating sanctions-related diligence as a comprehensive and ongoing undertaking throughout a business relationship. OFAC has repeatedly emphasized the importance of conducting sufficient sanctions-related due diligence when companies are considering a merger or acquisition or beginning a new business relationship. Even if a transaction involves only the acquisition of certain assets, companies should tailor their diligence to the full range of specific risks that are present. In this case, one type of risk—an acquisition target’s preexisting customer relationship with a blocked person—quickly gave rise to multiple apparent violations when the relationship continued post-acquisition.

Moreover, diligence should be redoubled in the presence of red flags. As this case demonstrates, entities encountering evidence indicating that a known counterparty is not the real or only interested party should work to identify sanctions-related risks, including that of dealing indirectly with a sanctioned person. Inconsistent explanations and questionable end-user representations are red flags that should be cause for particular concern. OFAC and its interagency partners have previously warned that sanctioned Russian parties often use third-party intermediaries to obscure their identities to evade U.S. sanctions and export controls.³

Relatedly, this case illustrates how ineffective oversight of foreign affiliates can create major risks for a U.S. parent company. Given the interconnected nature of many global businesses, risks that hatch abroad often come home to roost. Even entities with centralized or global sanctions compliance programs can be ensnared by the conduct of foreign affiliates who are either complicit in, or inattentive to, potential sanctions violations. To avoid this, companies should actively cultivate a strong culture of compliance across all operations globally. Particularly careful attention should be paid to affiliates who operate in or near high-risk jurisdictions such as Russia. The existence of compliance procedures alone is not sufficient where, as here, companies fail to follow those procedures or adequately investigate and resolve potential sanctions risks.

Finally, this case underscores the substantial benefits of voluntarily self-disclosing sanctions violations to OFAC. While OFAC considers the totality of the circumstances when determining how to address sanctions violations, voluntary self-disclosure generally reduces the likelihood that OFAC will seek a penalty, and—where a penalty is appropriate—the amount of any penalty, even when the agency determines conduct to be egregious.⁴

OFAC Enforcement and Compliance Resources

On May 2, 2019, OFAC published [A Framework for OFAC Compliance Commitments](#) (the “Framework”) 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

³ See Department of Commerce, Department of the Treasury, and Department of Justice, [“Tri-Seal Compliance Note: Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls”](#) (March 2, 2023).

⁴ See [OFAC Frequently Asked Question 13](#).

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 Enforcement Guidelines. 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>.

Whistleblower Program

The U.S. Department of the Treasury's Financial Crimes Enforcement Network maintains a whistleblower incentive program for violations of OFAC-administered sanctions, in addition to other violations of the International Emergency Economic Powers Act, the Foreign Narcotics Kingpin Designation Act, the Trading With the Enemy Act, and the Bank Secrecy Act. Individuals located in the United States or abroad who provide information about sanctions violations may be eligible for awards if the information they provide leads to a successful enforcement action that results in monetary penalties exceeding \$1,000,000. The incentive program is available for whistleblowers providing information relating to potential violations in any commercial sector.

For more information regarding OFAC regulations, please visit: <https://ofac.treasury.gov>.