



By: Tomorrow's Affairs Staff

The US company disclosed the sale to the sanctioned Russian missile factory just before journalists exposed it



US networking equipment manufacturer Extreme Networks has agreed to settlements announced on 27 October over its business with the Russian Avangard missile factory. OFAC, the US Treasury Department's financial sanctions agency, classified the case as an egregious offence.

As aggravating factors, it cited Extreme's reckless disregard of sanctions and warnings, which gave the company reason to know where its equipment was destined.

The deliveries covered by the proceedings lasted from March 2018 to March 2022, when Extreme closed its Russian office.

The company disclosed its dealings with Avangard to the US authorities in October 2022, a few days before the publication of the journalistic investigation, although it had received a whistleblower warning six months earlier.

OFAC recognised the report as voluntary and reduced the penalty as a result, while the Department of Justice determined that it was submitted too late to close the case without a plea deal.

Avangard produces missiles for Russia's S-300 and S-400 anti-aircraft systems, and Russia has also used **S-300 missiles** to attack ground targets in Ukraine.

Extreme supplied the factory with computer network equipment, along with software and support. Its products enabled the operation of the factory's IT systems and were not components of the missiles.

Avaya's contracts also brought a sanctioned customer

Extreme, a North Carolina-based company with more than 2,800 employees in 29 countries, had an office in Moscow with fewer than 15 people.

Some members of that small team concealed

the real buyer from the compliance department at the company's US headquarters.

Extreme's internal rules required compliance staff to review any business with Russia, so all disputed orders went through this review and were approved.

On 7 March 2017, Extreme agreed to acquire Avaya's networking business, then in bankruptcy reorganisation, for approximately \$100 million. The plea agreement does not name the seller, but **Extreme's filing** with the US Securities and Exchange Commission on the same day identifies it as Avaya.

The Russian part of Avaya's networking business transferred to Extreme in March 2018, along with contracts with existing customers. One of those contracts specifically named Avangard as the end user.

Avangard, referred to in the documents as MMZA, is majority-owned by Almaz-Antey, a state-owned group that is Russia's largest manufacturer of air defence systems, including the S-300, S-400 and Buk. The United States sanctioned Almaz-Antey in July 2014 over Russian intervention in Ukraine.

The **American ban** applies to companies on the sanctions list and to any company in which sanctioned persons collectively own at least half of the shares. Avangard was therefore already a prohibited customer when Extreme took over Avaya's contracts, although it was not listed separately until 28 June 2022.

OFAC does not allege that the director took part in a cover-up, but its findings show that the prohibited buyer also appeared in reports received by the company's regional management

Employees who knew the actual user were transferred along with the contracts. One of them, while the company was considering his employment, stated in an email that he had worked on the Almaz-Antey and Avangard

project at his previous employer.

Another, working at the distributor, directly assisted factory staff and took part in preparing Extreme's first order after the takeover. The change in ownership of the networking business left the existing relationship with the arms factory in the hands of the people who already managed it.

In an October 2022 filing with the regulator, Extreme also stated that a former employee, dismissed for poor performance, continued the same scheme after moving to a Russian distributor.

Four years later, in an agreement with prosecutors, the company accepted responsibility for the actions of its employees and representatives and for sales approved by its own departments.

The name Avangard was not confined to the Moscow office. In May 2018 and February 2019, Extreme's director for Northern and Eastern Europe, who oversaw staff in Russia, received regular reports on the office's activities that described dealings with Avangard.

OFAC does not allege that the director took part in a cover-up, but its findings show that the prohibited buyer also appeared in reports received by the company's regional management.

The equipment arrived under the name of an inactive company

Business records list DEMZ, a small firm from Dmitrov, north of Moscow, as the beneficiary. In an **investigation** published in 2022, its director, Vladimir Markov, said it had ceased trading in 2016. The individuals shown in Extreme's records as its executives were in fact Avangard employees using missile factory email addresses.

Extreme itself confirmed in its filing with the Securities and Exchange Commission that

DEMZ served as a front. The company's compliance staff therefore approved sales under the name of a company that, according to its director, had not traded for years. Seven of the nine purchase orders described by OFAC contained Avangard email addresses or the factory's Moscow address.

On 20 October and 10 November 2020, at the request of US staff, the distributor provided Avangard's website as the end user's address.

When the possibility of a military connection arose, it changed its answer, submitted the DEMZ web page and described the previous information as a mistake.

OFAC's findings cover nine export transactions, while the agreement with prosecutors lists 11 purchase orders

Extreme then approved the orders without further checks, accepting the word of the intermediary whose business it had just reviewed.

Support continued through Extreme's portal, where Avangard employees, following instructions from the Russian subsidiary, registered DEMZ as their company while retaining the factory email addresses.

Access was also granted to a user who failed to respond to a request for further details. Internal compliance allowed the relationship to continue even after the equipment was installed, when the manufacturer was dealing directly with staff at the factory.

OFAC's findings cover nine export transactions, while the agreement with prosecutors lists 11 purchase orders, two of which generated no revenue and related to software subscriptions and cloud services. Revenue from the transactions covered by that agreement was less than half a million dollars.

An internal investigation failed

to confirm the warning

The whistleblower submitted their report in April 2022, after the Russian office had closed. Extreme then launched an internal inquiry, but in a response to reporters in October it claimed the allegations came from a disgruntled employee and that it had found no corroboration.

The press inquiry, which included additional facts, came before the report to the US authorities, which the company submitted just days before publication.

Prosecutors later acknowledged that Extreme had made a good-faith effort to investigate the initial, incomplete allegations and had expanded the inquiry as it learned more, but that acknowledgement did not remove the consequences of the delay.

The fraud consisted of presenting an incorrect end user to the US authorities responsible for deciding whether exports were permitted

The company's inquiry failed to produce a report in time, even though information about Avangard was already contained in its own contracts, orders and reports.

Extreme has now pleaded guilty to conspiracy to defraud the United States, wilful violation of sanctions and export regulations, submission of false export information, and smuggling.

The fraud consisted of presenting an incorrect end user to the US authorities responsible for deciding whether exports were permitted. A deliberate cover-up was attributed to a group of employees in Russia, with the company held responsible for their actions.

Self-reporting did not bring the same outcome

For particularly serious violations, OFAC's rules set the starting fine at the legal maximum, which in this case was about \$3.4 million. By classifying the filing as voluntary, OFAC cut the initial amount in half, to about \$1.7 million, and the final settlement of \$1,529,685 is 10% lower than that.

As an aggravating factor, OFAC cited the damage to US foreign policy goals, and as mitigating factors it noted the changes made to the compliance system and the fact that the company had not previously faced proceedings before the agency.

Prosecutors evaluated the same facts differently. In deciding on the agreement, they took into account that the business was conducted by a small group of employees in the Russian subsidiary, that these employees actively concealed the business from US compliance staff, and that the income was less than half a million dollars.

The difference in the outcome stems from the separate rules of administrative and criminal procedure, which assess the same report and the same circumstances under different standards.

In the criminal proceedings, the maximum possible fine was twice the income from the prohibited activities. Prosecutors agreed to halve that amount, to about \$488,000, and confiscated as much as the company had earned on those contracts.

OFAC is counting part of that payment towards its settlement, so the company is paying a total of about \$2.02 million to both authorities.



Prosecutors have agreed not to prosecute Extreme if the company fulfils its obligations over the next three years – US Department of Justice

For the Department of Justice's **National Security Division**, this is the first resolution under the 2026 policy that allows companies that self-report late to avoid a criminal conviction, provided they fully cooperate and remediate their wrongdoing.

Prosecutors have agreed not to prosecute Extreme if the company fulfils its obligations over the next three years.

Under the agreement with **OFAC**, the company must maintain a compliance system for at least five years, and one of its senior executives must certify this in writing each year.

The agreement does not protect individuals, meaning that current and former employees can still be prosecuted.

The company handed over nearly 400,000 documents to investigators, provided translations and facilitated interviews with current and former employees, including those outside the US.

These documents enable prosecutors to determine who approved the disputed transactions, in which country they were approved and who is personally responsible for them.

The **policy** requires a company to report a violation before it faces the threat of public disclosure or a government investigation, and encourages it to come forward while its own inquiry is still under way.

Since even an inquiry conducted in good faith failed to secure Extreme the most favourable outcome, management can hardly justify waiting on the grounds that it first wanted to establish all the facts.

Corporate leaders who delay after a serious warning while completing their own checks will, in future, have to reckon with the possibility that an outsider, such as a journalist or whistleblower, may already hold the same documents and publish them before the company decides to contact the authorities.

A Russian missile factory received US equipment for four years because the company's compliance staff accepted a false end user and explanations that did not resolve obvious contradictions.

US authorities should require exporters to verify the customer while they are using the equipment and support, including in technical support tickets in which Avangard staff replied from their factory email addresses.

As long as fines remain at a level that a company with more than a billion dollars in annual revenue can absorb without serious consequences, the Russian arms industry will continue to seek access to Western equipment, specifically through exporters with the weakest controls.