Akin®

Treasury to Companies: Time to Take Ransomware Reporting Seriously

Dec 13, 2021

Reading Time : **8 min**

By: Natasha G. Kohne, Mahmoud (Mac) Fadlallah

On September 21, 2021, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) published an updated sanctions advisory, providing guidance to companies on sanctions compliance obligations related to ransomware payments. The bottom line: cyberattack victims should focus on defense and mitigation measures over a policy of paying out ransoms.[1]

The *Updated Advisory on Potential Risks for Facilitating Ransomware Payments* updates OFAC's prior guidance issued in October 2020. The new advisory reemphasizes self-reporting and highlights risks inherent in ransomware payments, while adding discussion of mitigating factors in enforcement actions. When self-reporting to OFAC, companies should note that agency officials will want as much detail as can be shared, including not just the victims and systems affected, but also how long the attacker was in those systems, the firms involved in the recovery, timeline of the attack, ransom amounts and ransomer information.

As mentioned in its latest guidance on virtual currency, OFAC is increasingly using its sanctions tools to target entities and individuals who use virtual currency in connection with malicious cyber activities. This guidance stresses the importance of the virtual currency industry's prioritization of cybersecurity and the need to implement effective sanction compliance controls to mitigate the risk of sanctioned persons exploiting virtual currencies and exchanges for ransomware demands.

OFAC can and will impose penalties on companies that elect to pay, or facilitate the payment of, ransomware money to sanctioned individuals and entities. Notably, OFAC recently designated on its Specially Designated Nationals and Blocked Persons List ("SDN List") two

virtual currency exchanges and associated individuals and entities for facilitating financial transactions involving ransomware actors. All U.S. persons globally are now prohibited from dealing with these newly sanctioned persons, including any assets they own or in their possession (virtual or otherwise).

OFAC Penalties and Mitigating Factors

Companies who fail to comply with the advisory may receive non-public penalties, such as No Action Letters or Cautionary Letters,[2] but OFAC may also impose strict liability monetary penalties. In the advisory, OFAC warns that companies that make payments to entities on the SDN List (or facilitate payments on behalf of a victim) may be held liable regardless of their knowledge of an entity's status on the SDN List.[3] More information about OFAC's economic sanctions enforcement can be found here.

Companies should take steps now to avoid OFAC's penalties. In the advisory, OFAC identifies three mitigating factors that decrease the likelihood that a company would face a civil penalty:

1. Implement a risk-based compliance program

OFAC suggests companies start with five key components: (1) support from senior management, including reviewing and approving the compliance program; (2) regular risk assessments that leverage information to create a "sanctions risk rating"; (3) internal controls that define reporting and escalation chains to relay information; (4) regular testing and auditing; and (5) personnel training that includes resources for recognizing high-risk entities and incidents.[4] For further guidance on compliance programs, OFAC has published a framework, available here.

2. Take anti-cyber extortion steps

The advisory points to the Cybersecurity and Infrastructure Security Agency's (CISA) September 2020 Ransomware Guide for guidance on establishing anti-cyber extortion practices. The guide advises that a company's first step should be to join an information sharing organization, such as the Multi-State Information Sharing and Analysis Center (MS-ISAC) or the Information Sharing and Analysis Organization (ISAO), followed by reaching out to CISA directly for additional information sharing and collaboration. Next, the company should begin building or evaluating ransomware best practices, such as implementing cybersecurity training programs, regularly updating anti-malware software and maintaining

offline backups. These best practices are considered "meaningful steps" to reduce the likelihood a company will face a ransomware attack.[5]

3. Self-report ransomware attacks

OFAC also encourages companies to self-report ransomware attacks, and notes that self-reporting is an important mitigating factor.[6] Reporting cyber events in general is an essential part of corporate governance. Companies should establish a format for prompt and complete reporting that includes technical details of the cyberattack such as which systems were accessed and the length of time the attacker had access. The victim company should also report as much information about the ransomer as possible, including the amount demanded, payment instructions and if payments were made to any sanctioned entities. Lastly, the company's ongoing cooperation is a vital component in this mitigating measure.

New Virtual Currency Guidance

On October 15, 2021, OFAC published new guidance on sanctions compliance related to dealings involving virtual currency. This guidance complements the ransomware advisory and provides an overview of U.S. sanctions for persons who may be unfamiliar (or need a refresher) on this area of the law. This guidance provides useful information on how transactions in virtual currency may trigger sanctions requirements, such prohibitions on dealing with blocked property, reporting requirements and penalties for noncompliance.

The content of this in the guidance will look familiar to those who have reviewed and implemented OFAC's May 2019 "A Framework for OFAC Compliance Commitments." Both documents encourage a risk-based approach to compliance and set out five essential components of a sanctions compliance program: (1) management commitment, (2) risk assessment, (3) internal controls, (4) testing/auditing, and (5) training. This guidance provides recommendations on each of these elements as it relates specifically to virtual currency.

Of particular relevance, OFAC underscores the need for companies dealing in virtual currency to assess early and often how sanctions requirements apply to their particular products and services—including, for example, requirements to block virtual currency held by blocked persons, adopting appropriate controls to screen for sanctions-specific risks (including through geolocation tools and reviewing IP addresses), and monitoring and investigating transactions involving suspicious virtual currency addresses. The guidance specifically calls out

ransomware payments as a particular area of concern given the increased use of virtual currency to facilitate transactions for ransomware actors.

Many operating in the virtual currency space have struggled with how to translate and apply rules that were designed based on a traditional fiat currency in the rapidly-growing virtual currency space. While the guidance does not expand sanctions compliance requirements applicable to virtual currency, it does provide a window into OFAC's expectations for companies that transact in virtual currency (including factors to be considered in implementing a sanctions compliance program) and OFAC's continued focus on the ways that virtual currency can be used to circumvent sanctions and undermine U.S. foreign policy interests and national security.

Recent Designations Relating to Ransomware Payments

The updated advisory pledges that OFAC will continue to sanction entities that "materially assist, sponsor, or provide financial material, or technological support" for ransomware attacks and transactions.[7] To this end, OFAC has added the virtual currency exchange SUEX to the SDN List, meaning U.S. persons globally that do business with this exchange, including any real or digital property that it owns or controls, may face significant penalties.

SUEX is a foreign virtual currency exchange that has facilitated payments for at least eight ransomware attacks, with over 40 percent of its transaction history associated with illicit actors.[8] OFAC has designated SUEX pursuant to Executive Order 13694 as amended, due to this material support for criminal ransomware actors.

This is the first time OFAC has placed a virtual currency exchange on the SDN List, and all companies, not just other exchanges, should take note. Virtual currency-based crimes like ransomware rely on exchanges like SUEX for their transactions with their cyberattack victims. OFAC adding exchanges to the SDN List may hinder ransomware criminals, but it may also have unfortunate repercussions for ransomware victims. This is because if the exchange the victim used to make a ransom payment has been sanctioned, then the victim could be subject to penalties.

Similarly, in a press release from November 8, 2021, OFAC announced that it had designated Russian citizen Yevgeniy Polyanin, his firm IP Polyanin, and Ukrainian citizen Yaroslav Vasinskyi for their involvement in ransomware attacks by the Sodinokibi/REvil group on U.S. government and private entities including the July attack on the IT company Kaseya. The

Treasury also announced having designated Chatex—a virtual currency exchange operating in multiple countries including Latvia and Estonia—for facilitating transactions for "ransomware actors." The Treasury took steps to designate the three entities registered in Latvia, Estonia and Saint Vincent and the Grenadines for providing support to Chatex.

The Treasury said it "benefitted immensely" from coordinating today's action with Latvian and Estonian authorities and stressed that international partnerships enhance its "ability to detect and disrupt, across continents and technologies, the illicit financial activities." Complementing the Treasury's action, the Department of State today announced rewards for information on Sodinokibi/REvil's leadership and for information leading to the arrest and/or conviction of participants in the group's ransomware attacks. As with the Chatex and SUEX designations, U.S. persons and financial institutions that engage in business transactions with these entities, including any real or digital property that it owns or controls, may face significant penalties or be subject to an enforcement action.

Key Takeaways

Companies should exercise caution when considering paying ransoms in response to cyberattacks, as doing so may result in larger unforeseen consequences due to U.S. sanctions. Compared to the October advisory, this recently issued advisory places greater emphasis on the need to thwart ransomware attacks by not only pursing perpetrators, but also individuals and companies who add fuel to this practice by making and facilitating ransomware payments. Companies should heed this guidance and structure their incident response plans to make reporting ransomware and other cyber events a key component of their corporate governance.

This updated advisory is also part of a larger pattern of the U.S. government strengthening its stance on ransomware reporting. A bipartisan bill introduced in September, the Cyber Incident Reporting Act of 2021, would require most businesses with 50 or more employees to report a ransomware payment to CISA within 24 hours. Another bill introduced in October, the Ransom Disclosure Act, would set the deadline at 48 hours and apply to organizations of any size. While it is uncertain what legislative response Congress will ultimately take, ransomware is certain to remain a substantial concern. The updated advisory from the Treasury and language from Congress indicate that more elements of cybersecurity are maturing in the regulatory space. Companies can look forward to tailoring their cybersecurity policies around more specific requirements from the federal government in the near future.

Please contact a member of Akin Gump's cybersecurity, privacy and data protection team if you have any questions about how the OFAC advisory or other Treasury actions may impact your company or your company's data privacy and cybersecurity programs.

---

[1] U.S. Dept. of the Treasury, *Updated Advisory on Potential Risks for Facilitating Ransomware Payments* (Sept. 21, 2021) ("Advisory"), available at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

[2] OFAC sends "No Action Letters" when OFAC finds a violation has not occurred or does not rise to the level of warranting an administrative response. The more serious "Cautionary Letters" are sent to communicate concerns to a subject when the subject's conduct may become a violation, or when the subject is not exercising due diligence, and a civil monetary penalty is not warranted. Appendix A to Part 501, Part II(A)-(C).

[3] *Id.*

[4] U.S. Dept. of the Treasury, *A Framework for OFAC Compliance Commitments*, (May 2, 2019), available at https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.

[5] Advisory at 4.

[6] *Id.* at 5.

[7] *Id.* at 3.

[8] Press Release, U.S. Dept. of the Treasury, Treasury Takes Robust Actions to Counter Ransomware (Sept. 21, 2021) available at https://home.treasury.gov/news/press-releases/jy0364.

Categories

Ransomware

OFAC