

U.S. Treasury Playing Hardball to Counter Ransomware Attacks: Be Wary of the Risks of Paying Ransoms or Facilitating Ransom Payments

September 30, 2021

On September 21, 2021, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) issued an [Updated Advisory](#)^[1] reminding and clarifying that it may seek sanctions against those who facilitate ransomware attacks, and those who make or facilitate ransom payments to cyber criminals and malicious cyber actors that OFAC has designated under its cyber-related sanctions program and other sanctions programs.

In addition, on the same day, OFAC added a Russian virtual currency exchange, SUEX OTC, S.R.O. (SUEX), to its Specially Designated Nationals and Blocked Persons List (the SDN List), because of SUEX's role in facilitating ransomware payments in the form of cryptocurrency.^[2]

These announcements signal that U.S. authorities are serious about aggressively countering ransomware attacks. While ransom payments continue to be discouraged, OFAC's Updated Advisory provides guidance on mitigating the risk of sanctions for those that pay ransoms.

Ransomware Attacks on the Rise

According to OFAC's Updated Advisory, there was a 21% increase in reported ransomware attacks and a 225% increase in ransomware-related losses from 2019 to 2020. Ransomware criminals don't discriminate—with attacks being carried out against small companies, non-profits and charities, government agencies, school districts, critical infrastructure organizations such as hospitals, as well as large global companies in key industries. Fueling this increase in such attacks is the advent of Ransomware for Hire (also known as Ransomware as a Service (RaaS)), in which criminals pay to obtain and use ransomware technology developed and leased by cyber-criminal gangs, thus making it accessible to anybody with an appetite for criminal and malicious extortion. As this RaaS industry has increased, so too has the frequency of ransom demands and payments, with total reported payments reaching over \$400 million in the U.S. in 2020, according to OFAC.^[3] The average ransom demand in the first half of 2021 was reportedly up to \$570,000 from an average of \$312,000 in 2020.^[4] In two high profile cases in the past year, Colonial Pipeline paid a ransom of \$5 million and JBS SA, the world's largest meat supplier, paid an \$11 million ransom. And the ransom costs are typically only a small fraction of the total costs to organizations from such attacks.

OFAC Updated Advisory on Ransomware

OFAC's Updated Advisory, which supersedes its [October 2020 Advisory](#),^[5] explains some of the aggressive actions OFAC is taking to curb the activities of cyber criminals and provides proactive steps that entities can take to mitigate the risk of being victimized by ransomware attacks.

One of the primary actions by OFAC has been to designate several cyber entities under its cyber-related sanctions program and other sanctions programs, including its SDN List. OFAC has designated foreign criminal organizations known to have perpetrated cyberattacks, as well as entities that support and facilitate such attacks. U.S. persons are generally prohibited from engaging in or facilitating transactions with entities and individuals that have been designated on OFAC sanctions lists or those located in embargoed and sanctioned countries and regions (such as Cuba, Iran, North Korea, and the Crimea region of Ukraine).

While the U.S. government has openly discouraged the payment of ransoms to ransomware criminals, it warns that it may now impose civil penalties based on strict liability if such payments are made to an entity or person designated under one of its sanctions programs. OFAC may take enforcement action against those ransomware victims that pay ransoms to listed persons or entities and against those that facilitate such payments, including cyber insurance providers, cybersecurity forensics and incident response firms, and financial services firms that process ransom payments. OFAC indicates that this aggressive step is warranted because often ransomware payments are used to fund other criminal activity and activities that threaten national security and U.S. foreign policy, such payments incentivize additional attacks, and the payments do not guarantee that the criminals will restore access to lost or frozen data or prevent further attacks.

As a way to avoid or mitigate the risk of ransomware attacks, OFAC suggests that entities do the following:

- Implement a risk-based sanctions compliance program with procedures to minimize and avoid transactions with entities or individuals on sanctions lists.
- Implement a robust cybersecurity compliance program, which includes cybersecurity training, incident response plans, authentication protocols, and antivirus and anti-malware software.
- Self-report ransomware attacks as soon as possible to law enforcement and other appropriate U.S. government agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA) and Treasury Department's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP). The contact information for the relevant federal agencies is included in the Updated Advisory.
- Cooperate fully with law enforcement and other government agencies, sharing all relevant information.
- If a ransom payment to a sanctioned entity is contemplated, apply to OFAC for a license to engage in a transaction that otherwise would be prohibited.

OFAC indicates in its Updated Advisory that these actions will be considered mitigating factors in deciding on any enforcement action, while also increasing the likelihood of recovering data that was lost or frozen, holding cyber criminals accountable, and preventing future attacks.

OFAC Designates Virtual Currency Exchange

On the same day that OFAC issued its Updated Advisory, it designated to the SDN List a virtual currency exchange, SUEX, for its role in facilitating ransomware transactions. This is first time a virtual currency exchange has been so designated and reflects a focus by OFAC on entities and individuals that facilitate criminal ransomware transactions. OFAC noted that virtual currency exchanges are critical to the execution of ransomware and other cybercrimes because virtual currency is the primary currency for ransomware demands and payments and associated money laundering and other cybercrime activities.

SUEX is a Czech-registered company that operates in Russia. OFAC found that over 40% of its historical transactions have involved illicit actors, including proceeds from at least eight ransomware variants. As a result of this designation, all property and interests of SUEX that are subject to U.S. jurisdiction are blocked, as are property and interests of entities owning 50% or more of SUEX, and U.S. persons and entities are prohibited from engaging in transactions with SUEX.

Insights

- OFAC and the U.S. government are serious about curbing ransomware attacks and will take action against those entities and individuals that facilitate such attacks. Financial institutions, virtual exchanges, and other entities involved in processing or receiving ransomware payments should have a sanctions compliance program which includes procedures to assess how their services are being

used and by what entities in order to ensure that they are not involved in facilitating ransomware payment transactions. Entities should implement effective customer due diligence (CDD) and know your customer (KYC) processes and procedures.

- Ransomware victims may decide that paying ransoms is necessary or advisable to avoid the costs and burdens of business disruptions associated with a ransomware attack. However, victims of ransomware attacks and those that advise victims on such payments, including insurance companies and cybersecurity forensics and incident response firms, should ensure that ransom payments are not being made to entities or individuals that are designated on the OFAC lists. This can be checked at <https://sanctionssearch.ofac.treas.gov/>. If a ransom payment to a sanctioned entity is contemplated, apply to OFAC for a license to engage in a transaction that otherwise would be prohibited.
- Victims of ransomware attacks should self-report attacks in a timely manner to, and cooperate fully with, applicable government agencies and law enforcement.
- Victims should consider whether they should disclose ransomware attacks to the public and whether there are any data breach reporting obligations.
- All entities should implement a comprehensive cybersecurity program designed to prevent cyberattacks and mitigate damage from such attacks. This program should involve training and procedural and technological safeguards.

Conclusion

If you have any questions about or need assistance in connection with ransomware, OFAC's policies and applicable laws, implementation of organizational cybersecurity programs and incident response plans, breach reporting obligations, and cybersecurity compliance and best practices, it is recommended that you speak to a cybersecurity law attorney.

* * *

[1] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

[2] <https://home.treasury.gov/news/press-releases/jy0364>.

[3] <https://home.treasury.gov/news/press-releases/jy0364>.

[4] <https://www.infosecurity-magazine.com/news/ransomware-demands-surge-2021/>.

[5] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

Carter Ledyard & Milburn LLP uses Client Advisories to inform clients and other interested parties of noteworthy issues, decisions and legislation which may affect them or their businesses. A Client Advisory does not constitute legal advice or an opinion. This document was not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein. © 2021 Carter Ledyard & Milburn LLP.

related professionals

Matthew D. Dunn / Partner

D 212-238-8706

mdunn@clm.com