

*To Pay or Not To Pay: What New
Regulatory Activity Means for
Ransomware Victims*





Having trouble reading this email? [View it in your browser.](#)

SEPTEMBER 2021

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK
HARDY & BACON

To Pay or Not To Pay: What New Regulatory Activity Means for Ransomware Victims

New regulatory activity may help companies experience fewer ransomware attacks and could impact whether ransoms can be paid to threat actors. The activity includes guidance and sanctions by the Department of Treasury and a host of resources provided by the Health and Human Services Office for Civil Rights. This alert describes the activity, its impact on companies that experience a ransomware attack, and practical takeaways for in-house counsel.

DEPARTMENT OF TREASURY

Yesterday, Treasury issued a [press release](#) announcing the designation of SUEX OTC, a virtual currency exchange, to the Specially Designated Nationals and Blocked Persons List (SDN List). Treasury also issued an [Updated Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments](#).

By way of background, Treasury's Office of Foreign Assets Control (OFAC) is responsible for administering and enforcing sanctions against foreign countries, terrorists and other entities or individuals engaged in activities deemed to be a threat to U.S. national security or the U.S. economy. To that end, OFAC may levy civil and criminal penalties against U.S. companies that engage in financial transactions with entities on the SDN List. The SDN List is essentially a [searchable](#) list of bad guys you're not allowed to help or do business with. Treasury will sometimes update the SDN List to include criminal organizations engaged in ransomware attacks.

SUBSCRIBE

ARCHIVE

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's [Privacy and Data Security](#) capabilities, please visit [shb.com](#) or contact:



Al Saikali

*Chair, Privacy and Data
Security Practice*

305.358.5171

asaikali@shb.com

Treasury's Designation of SUEX to the SDN List

For the first time, Treasury has added a virtual currency exchange to the SDN List. Treasury believes SUEX has facilitated financial transactions for threat actors associated with at least eight ransomware variants. According to Treasury, more than 40% of SUEX's transactions are associated with illicit actors.

As a result of this SDN List designation, all SUEX property interests subject to U.S. jurisdiction are blocked, U.S. companies/persons are not allowed to engage in transactions with SUEX, and any entity in which SUEX owns a 50% or more stake is blocked.

Implications of Adding SUEX to the SDN List

The designation of SUEX to the SDN List will impact a ransomware victim's ability to pay a ransom to purchase a decryption key or prevent further distribution of stolen data. But the full extent of that impact is not clear. Typically, ransom payments are made directly to a threat actor's crypto wallet address, without the direct use of an exchange. So, on its face, adding SUEX to the SDN List may not impact most ransom payments. But there are deeper implications to consider.

Certain principles guide whether OFAC will sanction a ransomware victim following the payment of a ransom. First, the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA) prohibits U.S. persons from engaging in transactions, *directly or indirectly*, with individuals or entities on the SDN List or country/region embargoes. Second, OFAC can impose *civil* penalties for sanctions violations based on *strict liability*. So even if the victim did not know or have reason to know it was engaging in a prohibited transaction, it could face steep monetary penalties. Third, just because OFAC *could* pursue sanctions does not mean that it will. Companies that take advantage of the mitigating factors described in the Updated Advisory discussed below will significantly decrease their risk.

So let's apply these principles to some potential scenarios:

SCENARIO 1

A ransom payment requires use of SUEX's exchange services; the victim nevertheless pays the ransom. A ransom payment here would *not* be permitted (at least not without a license from OFAC, the application for which OFAC will presumptively deny) because it would provide a direct benefit to an entity on the SDN List. The victim would face a high risk of civil *and criminal* penalties.



Colman McCarthy

Partner

816.559.2081

cdmccarthy@shb.com

SCENARIO 2

Due diligence provides a strong reason to believe the threat actor is using SUEX's exchange services as part of the threat actor's criminal activities (i.e., there is an indirect benefit to SUEX by paying the ransom); the victim nevertheless pays the ransom. This scenario presents significant risk. While the ransom payment is not benefitting SUEX directly, there is a high likelihood of an *indirect* benefit to the organization. Companies with a low risk tolerance for criminal or civil penalties will *not* pay the ransom under this scenario.

SCENARIO 3

Due diligence does not identify a reason to believe the SUEX exchange will receive a direct or indirect benefit from a ransom payment; the threat actor is not believed to have ties to SUEX; the victim pays the ransom; the due diligence later turns out to be *incorrect*. This scenario likely does not present the risk of criminal penalties (given the due diligence conclusions), but there is still a risk of civil penalties and a public relations nightmare associated with any public enforcement by OFAC.

SCENARIO 4

Due diligence leads to same conclusion as scenario 3; the victim pays the ransom; due diligence turns out to be *correct* in the long term. This is the only scenario that presents no real risk of sanctions, but it assumes thorough due diligence is performed and that you have a crystal ball allowing you to know at the time the due diligence is performed that the threat actor will not later use the ransom payment to benefit SUEX.

The "closer cases" in scenarios 2 and 3 are where the second Treasury development (an advisory explaining how companies can mitigate sanctions risks, explained below) is incredibly important.

Impact on Other Cryptocurrency Exchanges

Before we get to the advisory, one other implication of Treasury's decision is the impact to other virtual cryptocurrency exchanges. For now, the impact appears minimal. Treasury's press release states that SUEX was targeted because the company has allegedly "facilitate[d] illicit activities for their own illicit gains" and was not simply exploited by malicious actors (as is the case with other cryptocurrency exchanges). But given the scourge that ransomware has become in recent years, further actions against other exchanges is not outside the realm of possibility. If we were general counsel for a cryptocurrency exchange, we would implement as many measures as possible to proactively

identify/vet the use of our service by known or knowable ransomware threat actors. This is, unfortunately, much more difficult than it sounds given the inherent nature of cryptocurrency.

Treasury's Updated Advisory

The second development from Treasury was the issuance of an Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. The Advisory is a “must read” for all in-house counsel. It is a quick read and provides a good overview of OFAC's position on ransom payments. Most significantly, it provides companies a roadmap to avoid or minimize penalties for making a payment that results in a direct or indirect benefit to an entity on the SDN List.

First, your organization needs to implement certain security safeguards that reduce the risk of extortion. Those safeguards are highlighted in the Cybersecurity and Infrastructure Security Agency's (CISA) September 2020 Ransomware Guide and are familiar to those of us who counsel clients on ways to mitigate ransomware and other cybersecurity risks:

- maintain *offline* backups of data, which will increase your ability to restore data without the need to purchase a decryption key;
- develop an incident response plan, which will decrease operational downtime during a response, increase the speed of notification to regulatory authorities and law enforcement, and anticipate operational, legal and communication issues that arise during a ransomware attack;
- institute cybersecurity training, which will decrease the likelihood of human errors that lead to ransomware attacks (e.g., clicking on malicious links in emails, poor password hygiene or using non-sanctioned electronic devices and peer-to-peer networks);
- regularly update antivirus and anti-malware software, which will identify and contain many known malware threats. We would add that companies should definitely install an endpoint detection-and-response tool that monitors your network and endpoints for suspicious behavior; and,
- employ multifactor authentication protocols, which essentially eliminates the risk of compromised account credentials being used to obtain unauthorized access to a company's network.

Second, your organization must inform federal law enforcement and other relevant government agencies about the ransomware incident as soon as possible. Specifically, the Advisory states that, “[i]n the case of ransomware payments that may have a sanctions nexus, OFAC will consider a company's self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies, such as CISA or the U.S.

Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), made as soon as possible after discovery of an attack, to be a voluntary self-disclosure and a significant mitigating factor in determining an appropriate enforcement response."

Informing the FBI is a quick and easy process. You can do it using [this form](#). Most of the time you'll receive no response, but at least you have "checked the box" from a compliance perspective and helped law enforcement from a public-good perspective. Another option is to leverage your or your counsel's relationship with FBI or Secret Service Special Agents (this is not the preferred approach). Joining your local [InfraGard](#) chapter is a good idea as a way to develop relationships with the FBI and learn more about ransomware threat minimization techniques. Regardless of how you notify law enforcement, include legal counsel in the notification process and maintain a written record of the report. You'll need that record to demonstrate compliance to regulatory authorities and for any applicable insurance reimbursement.

Simply *informing* law enforcement is not enough. OFAC wants you to engage in "full and ongoing cooperation with law enforcement both during and after a ransomware attack — e.g., providing all relevant information such as technical details, ransom payment demand, and ransom payment instructions as soon as possible."

Finally, the Advisory states that "[v]ictims should also report ransomware attacks and payments to Treasury's OCCIP and contact OFAC if there is any reason to suspect a potential sanctions nexus with regard to a ransomware payment." Outside counsel will have the right point of contact for both offices and should work with you to prepare your submission.

The Advisory concludes that "[w]hile the resolution of each potential enforcement matter depends on the specific facts and circumstances, OFAC would be more likely to resolve apparent violations involving ransomware attacks with a non-public response (i.e., a No Action Letter or a Cautionary Letter) when the affected party took the mitigating steps described above, particularly reporting the ransomware attack to law enforcement as soon as possible and providing ongoing cooperation."

HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS

On the tail of the Treasury development, HHS issued a bulletin providing links to approximately 30 resources that covered entities and business associates should consult to help prevent, detect and mitigate ransomware attacks. The resources include

threat briefs that provide helpful information about specific threat actor groups, sector alerts regarding types of threats that have impacted HIPAA-governed entities, and updates about publicly known vulnerabilities. Most of those resources can be found on the [HHS website](#), and you can contact anyone on Shook's [Privacy and Data Security Team](#) for the full bulletin.

PRACTICAL TAKEAWAYS

What can in-house counsel take away from the Treasury and OCR developments?

- Ransomware victims who are considering making a ransom payment should work with legal counsel and other third-party professionals to perform due diligence into whether the payment will benefit the SUEX virtual cryptocurrency exchange.
- Ransomware victims that engage in financial transactions directly or indirectly benefitting SUEX cryptocurrency face the risk of civil and potentially criminal sanctions.
- Gather your information security leadership, ideally in coordination with counsel, to discuss your company's compliance with the proactive security recommendations in CISA's 2020 Ransomware Guide.
- Amend your incident response plan to include law enforcement and relevant regulatory notification processes/contacts.
- Incorporate discussion of law enforcement and regulatory notification into your tabletop exercises.
- Provide a copy of the HHS resources to your information security team and schedule quarterly (or even monthly) discussions to learn more about what your organization is doing to minimize these threats.

SHB.COM

ATLANTA | BOSTON | CHICAGO | DENVER | HOUSTON | KANSAS CITY | LONDON
LOS ANGELES | MIAMI | NEW YORK | ORANGE COUNTY | PHILADELPHIA
SAN FRANCISCO | SEATTLE | ST. LOUIS | TAMPA | WASHINGTON, D.C.

The choice of a lawyer is an important decision and should not be based solely upon advertisements.

© Shook, Hardy & Bacon L.L.P. All rights reserved.

[Unsubscribe](#) | [Forward to a Colleague](#) | [Privacy Notice](#)