CLIENT ALERT

OFAC Issues Updated Guidance on Ransomware Attacks and Imposes First Sanctions Designation on a Virtual Currency Exchange

Sep.28.2021

On September 21, 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued an updated advisory on potential sanctions risks for companies that facilitate ransomware payments in response to cyberattacks, guidance on preventative measures companies can implement to mitigate such risks, and criteria that OFAC will consider as mitigating factors in any potential enforcement action. OFAC also announced that it has added SUEX OTC, S.R.O. ("SUEX"), a Russian virtual currency exchange, to its Specially Designated Nationals and Blocked Persons List (the "SDN List"), as a result of its role in facilitating ransomware payments. This represents OFAC's first-ever designation of a virtual currency exchange.

These announcements come nearly a year after OFAC and the Financial Crimes Enforcement Network ("FinCEN") released concurrent advisories on the financial crime-related and sanctions-related risks associated with ransomware and ransomware payments. OFAC's new advisory supersedes and replaces its 2020 ransomware advisory. Although the updated advisory states that the U.S. government "strongly discourages" the private sector from paying ransomware demands, it provides guidance on methods of mitigating sanctions enforcement risk for those who elect to make such payments.

OFAC'S Updated Ransomware Advisory

OFAC's updated advisory continues to emphasize that facilitating ransomware payments may enable sanctioned individuals and those located in sanctioned jurisdictions to advance illicit activity, and that U.S. persons and those subject to U.S. jurisdiction may be subject to civil penalties for dealing with sanctioned persons in connection with such attacks. This includes non-U.S. persons that "cause" a U.S. person to violate the International Emergency Economic Powers Act ("IEEPA"), as well as U.S. persons that facilitate transactions by a foreign person with a sanctioned party that a U.S. person could not engage in directly. OFAC specifically identifies financial institutions—including virtual currency exchanges—cyber insurance firms, and digital forensics and incident response companies, as parties potentially subject to liability for facilitation. OFAC goes on to note that it "may impose civil penalties for sanctions violations based on strict liability," without any requirement that a violator knew of or intended any sanctions violation

At the same time, OFAC identifies a number of ways in which ransomware victims and those who assist them can prevent or mitigate sanctions enforcement.

First, OFAC encourages companies to implement risk-based sanctions compliance programs, noting its previous guidance that the existence and adequacy of such programs can be a mitigating factor against enforcement, and on the expected elements for such programs. OFAC also notes its expectation that the sanctions compliance programs for financial institutions and other companies that deal with ransoms for cyberattacks will specifically address the risk that a ransomware payment may violate sanctions.

Second, OFAC says that it will now treat "[m]eaningful steps taken to reduce the risk of extortion by a sanctioned actor through adopting or improving cybersecurity practices" as a "significant mitigating factor" in any OFAC enforcement analysis. These include measures such as those published in the Cybersecurity and Infrastructure Security Agency's ("CISA's") September 2020 Ransomware Guide. Specific cybersecurity measures include, among others: "maintaining offline backups of data, developing incident response plans, instituting cybersecurity training, regularly updating antivirus and anti-malware software, and employing authentication protocols."

Third, consistent with its 2020 ransomware guidance, OFAC will treat a timely and complete report of a ransomware attack to appropriate law enforcement agencies, along with complete cooperation during and after an attack, as mitigating factors against enforcement. In particular, OFAC says that, in 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." OFAC identifies the Federal Bureau of Investigation ("FBI") and the U.S. Secret Service as examples of appropriate law enforcement agencies. OFAC also says that victims "should" contact OFAC "if there is any reason to suspect a sanctions nexus with regard to a ransom payment."

With regard to mitigation for full and complete cooperation, such cooperation should include providing all relevant details of the cyber-attack, the ransom demand, and ransom payment instructions. According to OFAC, timely notification, full and complete cooperation with law enforcement, and sufficient pre-attack cybersecurity measures are more likely to result in a non-public action from OFAC, such as a Cautionary Letter or No Action Letter. However, any enforcement outcome will depend on the specific facts and circumstances.

OFAC's updated advisory makes no change to OFAC's previous position with respect to licensing and ransomware payments. OFAC will review license applications involving ransomware payments on a case-by-case basis, with a presumption of denial.

OFAC's Designation of SUEX and Treasury's Assessment of the Virtual Currency Sector

OFAC's designation of SUEX—and associated Bitcoin, Ether, and Tether wallet addresses—was based on analysis indicating that SUEX "facilitated transactions involving illicit proceeds from at least eight ransomware variants," and that over 40% of SUEX's known transactions involved illicit actors. OFAC designated SUEX pursuant to Executive Order 13694, which authorizes sanctions on persons who have participated in malicious cyber-enabled activities that constitute a significant threat to U.S. national security and foreign policy. As a result of this designation, all of SUEX's property interests subject to U.S. jurisdiction are blocked, and U.S. persons are prohibited from engaging in transactions with SUEX absent an applicable license from OFAC.

Treasury stated that certain virtual currency exchanges are "a critical element of [the ransomware] ecosystem, as virtual currency is the principal means of facilitating ransomware payments and associated money laundering activities," while acknowledging that most virtual currency activity is lawful. Still, Treasury claimed that virtual currencies can be used for illicit activities, such as facilitating sanctions evasion, ransomware schemes, and cybercrimes. Treasury explicitly stated that participants in the virtual currency sector have a "critical role" in sanctions compliance, anti-money laundering ("AML") efforts, and countering the financing of terrorism.

Key Takeaways

OFAC's updated advisory and the SUEX designation provide some notable takeaways for companies to consider, especially financial institutions and other companies that assist ransomware victims.

First, the U.S. government continues to strongly discourage ransomware payments. To that end, OFAC will now focus, when considering appropriate enforcement for sanctions violations, on the cybersecurity practices of ransomware victims to determine whether they took sufficient preventative measures to prevent a cyber-attack. As we have previously discussed in the context of the Colonial Pipeline cyber-attack, proper cybersecurity measures, risk management, and crisis management planning are essential. Thus, companies should make sure they have reliable and comprehensive data backup procedures, which include regular testing of backup data, that encryption is properly utilized to protect data at rest, and that endpoint detection technology is deployed to spot and halt ransomware before it spreads. Useful preventative measures also include honing and practicing incident response plans to counter a ransomware attack, conducting sanctions diligence on the virtual currency wallet address of a threat actor, any intermediary financial institutions or other parties that may play a role in facilitating payment of the ransom and, if known, the ransomware payment recipient, as well as developing strategies in advance for potentially engaging with law enforcement and OFAC.

Second, OFAC continues to place substantial emphasis on timely reporting of ransomware attacks to law enforcement and full and complete cooperation both during and after a ransomware attack. OFAC's announced willingness to treat timely and complete disclosures to appropriate law enforcement or cyber agencies of ransomware attacks as a voluntary self-disclosure ("VSD") represents a further incentive for such reporting.

Third, OFAC is making a stronger warning that financial institutions and other companies that facilitate ransomware payments may be subject to sanctions enforcement to the extent that they facilitate dealings with sanctioned parties. Furthermore, OFAC's designation of SUEX suggests that virtual currency exchanges that process substantial volumes of transactions for ransomware perpetrators may themselves become the targets of OFAC sanctions designations. OFAC's SUEX designation suggests that Treasury may be at the beginning of a broader effort to disrupt the ability of cybercriminals to convert, or off-ramp, virtual currency into fiat currency. Virtual currency exchanges may wish to assess any indicia that their services are being used to aid such attacks, and assess their transactions with other exchanges or platforms known to receive ransomware payments, to avoid such consequences.

While OFAC's guidance provides some helpful options for mitigating potential sanctions enforcement, its continued policy to presumptively deny any licensing of ransom payments to attackers could put victims in a challenging situation if they report an attack with a sanctions nexus to OFAC before payment has been made.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Caroline E. Brown
Partner – Washington, D.C.
Phone: +1 202.624.2509
Email: cbrown@crowell.com

Laura Foggan

Partner – Washington, D.C.
Phone: +1 202.624.2774
Email: lfoggan@crowell.com

Carlton Greene
Partner – Washington, D.C.
Phone: +1 202.624.2818
Email: cgreene@crowell.com

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

David (Dj) Wolff
Partner; Attorney at Law – Washington, D.C., London
Phone: +1 202.624.2548, +44.20.7413.1368
Email: djwolff@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Maida Oringher Lerner
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2596
Email: mlerner@crowell.com

Alexander Urbelis
Senior Counsel – New York
Phone: +1 212.895.4254
Email: aurbelis@crowell.com

Anand Sithian
Counsel – New York
Phone: +1 212.895.4270
Email: asithian@crowell.com

Matthew B. Welling
Partner – Washington, D.C.
Phone: +1 202.624.2588
Email: mwelling@crowell.com

Rebecca Lennon Baskin
Associate – New York
Phone: +1 212.895.4206

Email: rbaskin@crowell.com