O'Melveny

Alerts & Publications

Treasury Issues New Guidance on Risks of Ransomware Payments

October 9, 2020

KEY CONTACTS

Greta Lichtenbaum
Washington, DC
D: +1-202-383-5249

Laurel Loomis Rimon
Washington, DC
D: +1-202-383-5335

Scott W. Pink
Silicon Valley
D: +1-650-473-2629

John Dermody
Washington, DC
D: +1-202-383-5306

David J. Ribner
Washington, DC
D: +1-202-383-5507

Braddock Stevenson
Washington, DC
D: +1-202-383-5261

Maxwell E. Loos
Washington, DC
D: +1-202-383-5340

Paras Shah
Washington, DC
D: +1-202-383-5208

The Treasury Department has issued two new advisories warning US persons and entities, including financial institutions, of the risks of making and facilitating ransomware payments. The FBI and Department of Homeland Security regularly advise hacking victims not to make ransom payments. Treasury's new guidance adds teeth to these admonitions by reminding financial institutions of their obligation to report payments made by the victims of ransomware attacks and emphasizing the US Government's willingness to impose penalties when ransomware payments run afoul of government rules. For ransomware victims, the guidance illustrates the difficulty of their position and reinforces the need to have strong cyber security controls. For financial institutions, the guidance reflects the awkward position they are in to the extent their own obligations may require actions that could significantly damage their customers' operations and reputation. In either case, companies and financial institutions should pay careful attention to these issues and consider developing internal policies for addressing them.

Background on Ransomware

Ransomware is a type of malicious software designed to block access to a computer system or data, often by encrypting data or programs. Ransomware schemes typically involve cyber actors encrypting a victim's data and then extorting payments from the victim in exchange for decrypting the information and restoring access. In recent years, ransomware attacks have increased in frequency, sophistication, and cost. According to the FBI's 2018 and 2019 Internet Crime Reports, reported ransomware cases increased by 37% and losses spiked by 147% annually from 2018 to 2019. During the COVID-19 crisis, the FBI's Internet Crime Complaint Center has reportedly seen a 300% increase in the number of daily complaints.

Federal Agency Advisories

On October 1, 2020, two agencies within the Treasury Department issued advisories warning financial institutions of the regulatory and compliance risks that arise when processing ransomware payments. The Office of Foreign Assets Control's ("OFAC") advisory addresses sanctions compliance, while the Financial Crimes Enforcement Network ("FinCEN") advisory addresses reporting requirements under the Bank Secrecy Act ("BSA"). The advisories reinforce recent guidance from the Department of Homeland Security, discussed below.

The OFAC Advisory

OFAC issued its advisory to highlight the sanctions risks associated with ransomware payments, not only for victims that make such payments but also companies that facilitate ransomware payments, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response.

OFAC regulations generally prohibit persons subject to US jurisdiction from engaging in direct or indirect transactions with individuals or entities on OFAC's Specially Designated Nationals and Blocked Persons List ("SDN List"), and with persons subject to the US embargoes on Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria. OFAC has a cyber-related sanctions program and has designated numerous malicious actors including perpetrators of ransomware attacks and facilitators of ransomware payments.

The OFAC advisory clarifies that US persons could face civil liability for sanctions violations when they engage with victims of ransomware to facilitate or, in the case of financial institutions, process payments that involve a prohibited transaction, even if the US person did not know or have reason to know it was engaging in a prohibited transaction.

The OFAC advisory, therefore, encourages both financial institutions and companies that engage with victims of ransomware attacks to implement risk-based compliance programs to mitigate exposure to sanctions-related violations. The advisory also explains that a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement, as well as full and timely cooperation with law enforcement, are "significant mitigating factors" in determining potential penalties in the event of a sanctions violation.

The FinCEN Advisory

The FinCEN advisory explains that financial institutions, including money service businesses, should remain alert to transactions involving ransomware attacks as part of their reporting obligations under the BSA. In particular, "[f]inancial institutions should determine if filing a SAR [Suspicious Activity Report] is required or appropriate when dealing with an incident of ransomware conducted by, at, or through the financial institution, including ransom payments made by financial institutions that are victims of ransomware." A transaction is "suspicious" if the transaction: (1) involves funds derived from illegal activity; (2) is designed to evade reporting requirements; (3) has no business or apparent lawful purpose, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including background and possible purpose; or (4) involves use of the financial institution to facilitate criminal activity.

According to the advisory, cyber attackers often demand ransomware payments in convertible virtual currency ("CVC"), including Bitcoin. However, ransomware perpetrators are increasingly turning to Anonymity-Enhanced Cryptocurrencies ("AECs"), or "privacy coins," which "reduce the transparency of CVC financial flows" to law enforcement. FinCEN and other agencies remain skeptical of AECs and have penalized companies that fail to implement effective compliance programs and conduct due diligence on their customers. For instance, in July 2017, FinCEN assessed a $110 million civil penalty against BTC-e, a virtual currency exchange, after the company facilitated ransomware payments on thousands of suspicious transactions without filing a single SAR.

The FinCEN advisory lists ten financial "red flag indicators" to assist companies in detecting, preventing, and reporting suspicious ransomware transactions. The red flags include a customer providing information about a ransomware attack; a customer has limited understanding of CVC yet conducts a large transfer; a customer conducts rapid trading, especially with AECs, with no apparent business purpose; and open source information links a CVC address to ransomware.

FinCEN did not differentiate between red flags that would indicate a person as a ransomware victim versus a ransomware perpetrator. Based on the guidance, financial institutions may be required to report on the activity of the victims of the illicit activity. In a previous advisory relating to victims of financial fraud, including elder abuse, FinCEN specifically stated that the victims of the fraud "should not be reported as the subject of the SAR." FinCEN did not include such language in its ransomware advisory. The interplay between the FinCEN and OFAC guidance documents complicates SAR procedures on subject information and account risk reviews. Financial institutions should consider the implications discussed below if they adjust their SAR filing procedures:

- Many institutions have policies that can lead to risk elevation or even account closure for customer-related SARs. Therefore, institutions should review those policies and have clear procedures for determining when a customer will be considered a subject for SAR-filing purposes.
- FinCEN previously exempted financial institutions from filing SARs for transactions, or attempted transactions, with SDNs so long as the institution filed a blocking report with OFAC and the transaction was not otherwise suspicious. As ransomware transactions may demonstrate additional suspicious activity beyond sanctions concerns, institutions should consider if certain activity, or attempted activity, will result in a dual reporting requirement to both OFAC and FinCEN.

Recent CISA Guidance

The OFAC and FinCEN advisories come on the heels of ransomware guidance issued on September 30, 2020 by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC), which explicitly states that federal law enforcement does not recommend payment of ransom in response to a ransomware attack.

The CISA guidance provides detailed technical recommendations to organizations for both preventing and responding to ransomware attacks, and includes a step-by-step ransomware response checklist intended to serve as a template that organizations can use to draft their own ransomware response plans. Notably absent from the response checklist are any steps regarding payment of ransom. The guidance instead provides a list of law enforcement agencies that victims of a ransomware attack should contact, noting that security researchers have already developed decryptors for several ransomware variants, and listing types of information about an attack that law enforcement may be interested in.

Implications

The OFAC and FinCEN advisories stress the need for companies to develop and update strong sanctions compliance and anti-money laundering programs in response to ransomware attacks. The guidance also highlights the need for companies to monitor and report suspicious activity to law enforcement and remain aware of the sanctions risks involved with processing ransomware payments, even when those payments are on behalf of ransomware victims.

The coordinated timing and the content of the advisories also suggest a coalescence among federal agencies—particularly those addressing national security issues—around a position of discouraging victims of ransomware attacks from paying the ransoms demanded of them. In 2016, for example, guidance from the FBI admitted that whether or not to pay a ransom after systems have been compromised is a "serious decision." By 2019, however, the FBI had shifted to urging victims not to pay ransoms to cybercriminals, and to instead contact a local FBI field office.

OFAC, CISA, and the FBI all note that payment of a ransom does not guarantee the release of stolen data, and that payment of ransoms may encourage future attacks and provide material support for activities adverse to US foreign-policy and national-security objectives. But the OFAC advisory represents the strongest official announcement that victims of ransomware attacks may also find themselves subject to government-imposed penalties for paying a ransom, on top of the costs of any ransom paid.

The fact remains that the best strategy for addressing ransomware is prevention and the development of policies and procedures for handling such events in advance. The newly issued guidance by OFAC and FinCEN, however, underscores the increasingly precarious legal tightrope that companies are forced to walk when faced with the threat of malicious actors holding data and systems hostage.

This memorandum is a summary for general information and discussion only and may be considered an advertisement for certain purposes. It is not a full analysis of the matters presented, may not be relied upon as legal advice, and does not purport to represent the views of our clients or the Firm. Greta Lichtenbaum, an O'Melveny partner licensed to practice law in the District of Columbia, Lisa Monaco, an O'Melveny partner licensed to practice law in the District of Columbia and New York, Laurel Loomis Rimon, an O'Melveny partner licensed to practice law in the District of Columbia and California, Scott Pink, an O'Melveny special counsel licensed to practice law in California, John Dermody, an O'Melveny counsel licensed to practice law in California and the District of Columbia, David J. Ribner, an O'Melveny counsel licensed to practice law in the District of Columbia and New York, Braddock Stevenson, an O'Melveny counsel licensed to practice law in New York and New Jersey, Maxwell E. Loos, an O'Melveny associate licensed to practice law in the District of Columbia, and Paras Shah, an O'Melveny associate licensed to practice law in New York, contributed to the content of this newsletter. The views expressed in this newsletter are the views of the authors except as otherwise noted.