PUBLICATION

New Ransomware Advisories from OFAC and FinCEN Create Additional Challenges for Financial Institutions

Authors: Matthew George White, Alexander Frank Koskey, III
January 06, 2021

Both the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN) of the U.S. Department of Treasury have issued advisories recently regarding regulatory considerations financial institutions should take into account when processing ransom payments. These advisories are especially noteworthy as we enter the new year. We saw a substantial increase in ransomware attacks during the COVID-19 pandemic and anticipate that they will continue in 2021. These attacks are also becoming more layered and sophisticated with cybercriminals gaining access to computer networks for extended periods of time.

The advisories include general guidance for financial institutions that are either (1) involved in making a ransom payment or (2) have reasonable knowledge that money is being used by a customer to make a ransom payment. It is this second aspect that adds another dimension of the responsibility on financial institutions they have not previously had to consider. OFAC and FinCEN warn financial institutions and payment intermediaries of potential sanctions risks involved in making ransom payments as well as provide information on requirements for Suspicious Activity Reports (SARs) under anti-money laundering regulations.

Financial institutions must be especially keen to these advisories both as a potential target of an attack and potential intermediary of a ransom payment involving a customer. In particular, financial institutions should be: (1) incorporating provisions into third-party vendor contracts to address OFAC compliance issues; (2) ensuring that appropriate red flag indicators are in place to detect, prevent and report suspicious transactions associated with ransomware attacks; (3) developing and refining protocols for filing a SAR related to a ransomware attack or payment; and (4) reviewing their incident response plans to address potential issues associated with ransomware attacks. Financial institutions must review and address these issues as soon as possible to reduce potential risk and be better prepared in the event of an attack or how to respond if there is reason to believe its customer is paying a ransom.

Rise of Ransomware Attacks

As explained by the Treasury, ransomware is a form of malicious software used by attackers to block victims' access to their computer systems or data, often through encryption. Malicious actors then extort a ransom payment in exchange for restoring access. These attacks can lead to severe consequences including the loss of data, the publication of proprietary information and the overall loss of business functionality. Malicious actors not only target large corporations but also small and medium-sized businesses, government agencies, hospitals and schools.

The rise in ransomware attacks in recent years has led to the creation of digital forensics and cyber insurance companies designed to assist victims with responding to ransomware attacks. Ransoms paid to malicious actors to regain access to systems or data are often paid through these companies and are usually paid in digital currency through a financial institution. When an intermediary facilitates the payments, they are usually required to register as money services businesses with FinCEN and are exposed to similar regulations as financial institutions. The processing of these payments therefore presents risks to the victim, the financial institution and any intermediaries.

Ransom payments are processed through complex financial pathways designed to mask the identity of the attacker. Consequently, paying the ransom may run the risk of the victim, the financial institution or the payment intermediary knowingly or unknowingly violating U.S. sanctions laws. Additionally, as ransoms become more and more costly, processing these payments may trigger financial institutions or money services businesses' requirement to file a SAR.

OFAC and FinCEN's recent advisories highlight the regulations faced by financial institutions and payment intermediaries when processing these payments in response to an attack or when facilitating victims' payments and provides guidelines in ensuring compliance and reducing risk.

Risks of Ransomware Payments and Guidelines to Follow

OFAC designates malicious actors as Specially Designed Nationals and Blocked Persons (SDNs), including both perpetrators of ransomware attacks and those who facilitate these attacks through materially assisting, sponsoring or providing financial, material or technological support for ransomware attacks.

OFAC warns in its advisory that U.S. persons are prohibited from directly or indirectly engaging in or facilitating transactions with SDNs or other blocked persons as well as with those covered by comprehensive country or region embargoes such as Cuba, the Crimea region of Ukraine, Iran, North Korea and Syria. Financial institutions and intermediaries involved in making payments as a victim of a ransomware attack or in processing other victims' ransom payments through their services must ensure that the entity to whom they are making a ransomware payment is not on a blocked persons list or located in or affiliated with an embargoed jurisdiction. OFAC warns that it may impose civil penalties under a strict liability standard for violations, meaning that it may impose civil penalties regardless of whether the person processing the payment knew or should have known that it was engaging in a transaction prohibited under sanctions laws.

When deciding the appropriate enforcement response, OFAC takes into account the adequacy of the violating party's sanctions compliance program. Therefore, OFAC recommends that financial institutions and other intermediaries such as cyber insurance, digital forensics and incident response services implement a strong risk-based compliance program to mitigate the company's exposure to potential sanctions violations. Compliance programs should account for the risk that a payment may involve a blocked person or a person or embargoed jurisdiction.

OFAC underlines in its advisory that making or facilitating ransomware payments with a sanctions nexus may enable malicious cyber actors to advance their goals. A ransomware payment made to a sanctioned person or a sanctioned jurisdiction, according to OFAC, may be used to fund activities adverse to national security, may embolden actors to continue to engage in ransomware attacks, and does not guarantee that the malicious actor will actually restore the victim's access to the encrypted data or systems.

If your institution is subject to a ransomware attack, financial institutions should ensure self-initiated, timely and complete reports of any ransomware attack to law enforcement as well as the Treasury's Office of Cybersecurity and Critical Infrastructure Protection. Additionally, if a financial institution or intermediary believes that a ransomware payment may involve a sanctions nexus, it should contact OFAC directly.

Detecting and Reporting Suspicious Ransomware Payments

FinCEN's advisory provides helpful guidance for financial institutions and money services businesses to better detect and report suspicious payments as required by FinCEN's anti-money laundering regulations. The advisory provides red flag indicators of illicit activity related to ransomware to assist institutions in preventing and detecting suspicious payments made by or through its institution. For example, these red flag indicators include transactions occurring between an organization from a high-risk sector (e.g., financial, government, educational, health care, etc.) and a digital forensics or cyber insurance company, transactions between a

digital forensics or cyber insurance company involving receiving funds followed by sending equivalent funds to a CVC exchange shortly after, and certain large CVC transactions that are out of the ordinary for that customer. For the full list of red flags, see the advisory here.

The FinCEN advisory also delineates reporting requirements that financial institutions and money services businesses must make when they suspect suspicious payment activity. FinCEN reminds financial institutions and money services business of their obligation under anti-money laundering regulations to report suspicious activity by filing SARs with FinCEN. According to FinCEN, SARs should be filed when a suspicious payment is made at or through the institution as well as when the institution is paying a ransom payment itself as victim of a ransomware attack. A financial institution or money services business is required to file a SAR if it knows, suspects or has reason to suspect that a transaction conducted *or* attempted by, at or through the institution involves illegal activity when the payment amounts, in one or multiple transactions, to $5,000 or more ($2,000 for money services businesses). FinCEN's advisory provides detailed information on how and where to file such reports as well as what type of information to include in these reports.

Pursuant to FinCEN's guidance, financial institutions and money services businesses should include protocols for detecting suspicious activity and for correctly filing SARs with FinCEN in their compliance protocols, taking into account FinCEN's red flag indicators.

Ransomware attacks are becoming more numerous, sophisticated and costly, especially during the COVID-19 pandemic. Pursuant to the Treasury's recent guidance, financial institutions and intermediaries should ensure that they have risk-based compliance programs in place for both sanctions risks and for detecting and reporting suspicious activity with regards to both payments made by the institution as a victim of a ransomware attack and ransom payments made by a customer at or through the institution.

These new advisories reinforce the importance of financial institutions doing tabletop exercises to simulate what to do in the event of a ransomware attack and/or how to respond when a suspicious transaction is identified involving a customer that may be paying a ransom. Simulating these scenarios – and evaluating the variety of different factors that could come into play – is a proactive measure that financial institutions can take to be prepared for when these issues arise in real time.

If you have any questions regarding the recent OFAC and FinCEN advisories, or any other aspect of ransomware attacks, please contact the authors or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.