Hughes Hubbard & Reed

U.S. Department of the Treasury Highlights Compliance Risks with Ransomware Payments

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

October 5, 2020 – On October 1, 2020, the U.S. Department of the Treasury issued two advisories regarding potential risks in making ransomware payments, highlighting another layer of complexity to this already dangerous and uncertain environment. The first advisory, issued by the Financial Crimes Enforcement Network ("FinCEN"), informs financial institutions and related entities of the potential money-laundering risks and related reporting obligations associated with ransomware payments. The second advisory, issued by the Office of Foreign Assets Control ("OFAC"), highlights the sanctions risks associated with making or facilitating ransomware payments. Both advisories, while offered as informational guidance, are designed to encourage early, if not immediate, engagement with law enforcement authorities when victimized by a ransomware attack.

What is Ransomware?

Ransomware is malicious software that blocks access to a computer system or data as a means to extort monetary payments from victims in exchange for restoring access to the system or data. Ransomware often works by encrypting the targeted files, and attackers may additionally threaten to sell or make public sensitive or embarrassing data if the payments are not made.

The advisories are timely, as ransomware attacks have proliferated and grown in sophistication. As observed in the OFAC advisory, according to the Federal Bureau of Investigation's 2018 and 2019 Internet Crime Reports, there was a 37 percent annual increase in reported ransomware cases and a 147 percent annual increase in associated losses from 2018 to 2019. While ransomware attacks often target large corporations, many ransomware attacks target small- and medium-sized companies across a range of industries.

FinCEN Advisory

The FinCEN guidance – entitled *"Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments"* – details that ransomware attacks typically require that the payments be made in convertible virtual currency ("CVC"), such as Bitcoin. The process of purchasing the CVC, executing the payment, and laundering the payment back into the financial system typically involves a multi-step process that includes at least one depository institution and one or more money services business ("MSB"). MSBs broadly include currency dealers or exchanges (including those for cryptocurrencies) and "money transmitters" involved in the transfer of funds.

Depending on the specific circumstances of a payment, these companies may have an obligation to, among other things, register as an MSB with FinCEN, comply with Bank Secrecy Act ("BSA") obligations, and/or file Suspicious Activity Reports ("SARs"). In particular, a covered business is required to file a SAR for any transaction above a *de minimis* threshold involving funds derived from or intended to hide illegal activity, evade the BSA, lack a business or other apparent lawful purpose, or otherwise facilitate criminal activity. Both successful and unsuccessful attempted payments must be reported.

The FinCEN advisory identifies several trends and typographies of recent known ransomware attacks, including:

- ***Big Game Hunting*** – attackers are targeting larger enterprises and demanding bigger payouts;
- ***Criminal Partnerships and Resource Sharing*** – some groups engaging in ransomware attacks are sharing resources, including ready-to-use "kits" that include malicious code and other tools;
- ***Double Extortion Schemes*** – attackers are identifying and removing sensitive or embarrassing data to demand a second payment to avoid publishing or selling the data;
- ***Use of Anonymity Enhanced Cryptocurrencies*** – increasingly, attackers are requiring or offering discounted demands if victims make their payments using crypto currencies designed to enhance digital anonymity, and therefore facilitate laundering the funds and evading detection; and
- ***Use of "Fileless" Ransomware*** – some ransomware groups are engaging in sophisticated attacks that write malicious code into a computer's memory, rather than load a file, making the attack more difficult to detect using off-the-shelf antivirus and malware software.

The FinCEN guidance also identifies several red flags that financial institutions should watch for, including:

- Suspicious activity in system log files, network traffic, or file information;
- Information provided during the creation of a new account suggesting that the account will be used to make ransomware payments;
- Customer use of a cryptocurrency address known to be linked to ransomware strains, payments, or related activity;
- Transactions between an organization at high risk for a ransomware attack and a digital forensics and incident responses ("DFIR") entity or cyber insurance company ("CIC");
- Payments to an account held by a DFIR or CIC followed by an outgoing payment in the same amount;
- Customer who shows little knowledge of cryptocurrencies, but requests their purchase, particularly in a large amount or on a rush basis;
- Customer who has little history of engaging in cryptocurrency transactions who engages in a large transaction involving cryptocurrencies;
- Customer who is not registered as an MSB with FinCEN engaging in a large number of offsetting cryptocurrency exchanges;
- Customer who uses a cryptocurrency exchange or non-U.S. MSB located in a high-risk jurisdiction; and
- Customer who engages in multiple, rapid transactions involving a cryptocurrencies, especially an Anonymity Enhanced Cryptocurrency.

OFAC Advisory

The OFAC guidance – entitled *"Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments"* – warns parties engaging in ransomware payments of the sanctions risks inherent in such transactions. Specifically, OFAC has identified numerous parties actively engaging in ransomware attacks who have been added to the Specially Designated Nationals ("SDNs") list under cyber-related sanctions authorities.

These include:

- Evgeniy Mikhailovich Bogachev, the developer of Cryptolocker, which has infected an estimated 234,000 computers starting in 2013;
- Ali Khorashadizadeh and Mohammad Ghorbaniyan, two Iranian nationals who helped exchange digital currency (Bitcoin) ransom payments into Iranian rial on behalf of Iranian malicious cyber actors involved with the SamSam ransomware scheme that targeted over 200 known victims in 2015;
- The Lazarus Group (a cybercrime group sponsored by North Korea), and two subgroups, Bluenoroff and Andariel, who used the ransomware program WannaCry 2.0 to infect approximately 300,000 computers in May 2017; and
- Evil Corp, a Russian cybercrime organization, and its leader, Maksim Yakubets, for developing and using the program Dridex to steal more than $100 million since 2015.

U.S. persons (including U.S. nationals, permanent residents, persons physically present in the United States, and entities organized under U.S. law) are prohibited from engaging in virtually all transactions involving SDNs or entities owned fifty percent or more by an SDN, whether directly or indirectly. Additionally, any transaction that "causes" a U.S. person to violate sanctions, or any transaction by a U.S. person to "facilitate" a prohibited transaction by a non-U.S. person, is prohibited.

The clear message in the OFAC advisory is that ransomware payments by U.S. persons or involving U.S. financial institutions carry a significant risk of violating U.S. sanctions. This risk is heightened when the identity of the party receiving the payment is unknown, and therefore unable to be adequately screened for exposure to sanctions. While OFAC reviews license requests to engage in prohibited ransomware payments on a case-by-case basis, it reviews these requests under a "presumption of denial." It is important to note that OFAC assesses fines and penalties on a strict liability basis, and even inadvertent and unintentional violations could be subject to civil enforcement. While the U.S. Department of Justice requires that violations be conducted with intent when bringing a criminal sanctions case, the requisite intent may be found in conduct that is "willfully blind" to the sanctions risks.

If a U.S. person believes that a ransomware payment may have been made to an SDN, the U.S. person may initiate a voluntary self-disclosure to OFAC as a means of mitigating its enforcement risks. OFAC gives significant weight to self-initiated disclosures in making enforcement decisions. Further, the advisory states that OFAC considers a company's full and timely cooperation with law enforcement to be a "significant mitigating factor" in making an enforcement decision.

Conclusion

Ransomware attacks are a growing threat to companies, especially those with potentially sensitive data. In the moments after an attack is discovered, companies may be tempted to quietly make the demanded payments to regain access to their data and avoid potential reputational harm. However, these payments should be approached with caution, as they may trigger, among other things, reporting obligations (by the victim or the victim's financial institutions) under the BSA or benefit a sanctioned party. The FinCEN and OFAC advisories make clear that ransomware attacks and an assessment of the victim's response, will be a focal point of the agencies' enforcement efforts. To avoid inadvertently violating applicable regulations, companies at risk of ransomware

attacks are therefore encouraged to create, implement, and test written protocols in advance of responding to ransomware attacks and ensure compliance with U.S. law.

Related People

Ryan Fayhee

Tyler Grove

Joshua Rosenthal

Related Areas of Focus

Sanctions, Export Controls & Anti-Money Laundering
Environmental, Social & Governance (ESG)