Overview

On October 1, 2020, the US Department of the Treasury’s Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN) published advisories on the sanctions and anti-money laundering (AML) risks of facilitating ransomware payments.

Ransomware attacks have become increasingly common in recent years with malicious attacks targeting companies in a variety of industries, including healthcare, technology, and education, among others. Ransomware attacks typically involve a hacker breaching a company's information technology (IT) infrastructure and encrypting a company's data or other systems. The attacker then typically demands the victim pay a ransom in exchange for a decryption key that allows the victim to unlock the IT systems or data. Such attacks can have severe consequences for the victim, often preventing the victim from being able to conduct business operations in whole or in part, and, in the case of healthcare companies such as hospitals, can potentially lead to loss of life, as reportedly occurred recently with a ransomware attack on a hospital in Germany. Such inability to conduct business can also have ripple effects on other companies or individuals whose data is affected. In some instances, an attacker may also threaten to disclose private information or data unless the ransom is paid.

As a result, victims of ransomware attacks often choose to pay the ransom. However, because ransomware attackers rarely, if ever, identify themselves, and often demand payment in cryptocurrency, victims making such payments are generally forced to do so without a clear understanding of the recipient. Such conduct potentially exposes the victim, and third-party service providers (including financial institutions and incident response consultants, among others), to violations of and obligations under US sanctions and/or AML laws, in addition to other sanction regimes around the world, such as those recently deployed by the European Union.[1]

The OFAC and FinCEN advisories provide information to the public regarding the sanctions and AML risks to victims and third-party service providers, including US financial institutions, who assist victims in responding to ransomware attacks. While in many respects the guidance does not break new regulatory ground, it is a stark reminder of the way that those trying to deal with the consequences of a ransomware attack can find themselves in trouble with the US government. This puts victims and companies that assist them in a difficult conundrum: don’t pay the ransom and potentially watch the victim company’s business get destroyed, or pay the ransom and run the risk of violating US sanctions and AML laws. It is therefore imperative that victim companies and those in the business of facilitating ransom payments carefully consider the legal risks and evaluate potential ways to avoid or minimize them.

1. Making or Facilitating Ransomware Payments May Violate OFAC Sanctions
The OFAC advisory notes that OFAC has designated a number of ransomware attackers as Specially Designed Nationals and Blocked Persons (SDNs). US persons are generally prohibited from dealing with SDNs. In addition, property and interest in property of SDNs must be blocked (i.e., frozen) when within the possession or control of a US person or within the United States, and must be reported by US persons to OFAC within 10 days after blocking. Entities owned 50% or more by one or more SDNs are subject to the same restrictions. Other attackers may not be included on the SDN List, but could be located in a jurisdiction subject to comprehensive US sanctions – currently, Iran, North Korea, Syria, Cuba, and the Crimea region of Ukraine – or could be affiliated with the governments of those jurisdictions, including any department, branches, state-owned enterprise, officers, or agents of the foregoing (and increasingly, Venezuela). Generally speaking, US persons cannot engage in transactions with entities or persons in such jurisdictions, including the governments of such jurisdictions (and their state-owned or controlled entities). There are no general licenses or exemptions available to US persons specific to ransomware attacks.

Dealings with SDNs and comprehensively sanctioned jurisdictions can also present risks to non-US persons when (1) their dealings have a US nexus, including use of the US financial system, which may “cause” a US person to violate sanctions, or (2) their dealings have no US nexus but are sanctionable under OFAC’s so-called “secondary sanctions” authorities, which target non-US persons who deal with SDNs, participate in specified industries in sanctioned countries, or support certain end uses of concern.

The OFAC advisory highlights that OFAC primary sanctions are a strict liability regime, meaning “that a person subject to US jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.” This strict liability regime can present significant complications for victims of ransomware attacks and those assisting victims, who are often unable to definitively determine the identity of the attacker.

The OFAC advisory further notes that “financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations.” It adds that “companies that engage with victims of ransomware attacks” should implement a “risk-based compliance program to mitigate exposure to sanctions-related violations” to “account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction.” Although it may be possible to identify the apparent jurisdiction of a ransomware attacker and/or where payments to the attacker are destined, this is not always the case given attackers’ ability to obfuscate their physical location. Likewise, it may be very difficult to develop a risk-based compliance program when dealing with individuals or entities whose identity may be unknowable, even after extensive diligence efforts. These risk-based compliance efforts are further complicated by the fact that victims of ransomware attacks, and the third parties who support them, are often given very little time to assess the situation and make a determination regarding how to respond.

2. OFAC Encourages Victims to Report Ransomware Attacks

OFAC’s advisory notes:

Under OFAC’s Enforcement Guidelines, OFAC will also consider a company’s self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus. OFAC will also consider a company’s full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.

OFAC seems to acknowledge the difficulty in obtaining certainty regarding the identity of ransomware attackers and indicates that it will take that difficulty into account so long as a self-initiated, timely, and complete report is made to law enforcement. OFAC’s enforcement guidelines, including other enumerated mitigating and aggravating factors, are available here.

However, it is unclear if such mitigation credit is available only when “the situation is later determined to have a sanctions nexus” (emphasis added) as the first sentence quoted above indicates, as opposed to situations in which a sanctions nexus is known or suspected prior to making the payment. The second sentence in the quoted language suggests that as long as there is cooperation with law enforcement “during and after” the attack, OFAC will take that into account. On the other hand, OFAC would typically expect any person knowingly dealing with an SDN or other blocked person to apply for a specific license (i.e., written approval), regardless of any exigent circumstances, unless a general license or regulatory exemption exists.

3. License Applications for Payments to Sanctioned Actors Subject to Presumption of Denial
In situations in which a party wishes to engage in conduct that would otherwise be prohibited, it is possible to request a specific license from OFAC authorizing such conduct. However, OFAC’s guidance states “license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial.” This suggests OFAC will not generally approve license applications for ransomware payments to sanctioned persons, but may approve a license in certain limited instances depending upon the facts and circumstances.

The guidance also states, “OFAC encourages victims and those involved with addressing ransomware attacks to contact OFAC immediately if they believe a request for a ransomware payment may involve a sanctions nexus.” OFAC’s licensing policy and request that parties contact OFAC as soon as a potential sanctions risk is identified has the potential to create a difficult bind for companies. OFAC often takes weeks if not months to respond to license requests. Such delay may be manageable in a normal commercial context where business transactions can be scheduled to take into account the long license application processing times of OFAC. This typically is not the case, however, for a victim dealing with a ransomware attack that could have immediate and devastating business consequences for the victim and longer lasting liability and reputational consequences. Moreover, as a recent ransomware attack on a German hospital reportedly shows, ransomware attacks can even threaten human life in some instances in the case of healthcare providers, if not addressed in a matter of hours. It is possible OFAC would fast-track such license applications, but it did not explicitly state this contingency in the advisory. But even an administrative fast track may not be fast enough to prevent severe consequences.

A further complication may exist in situations in which the connection to a sanctioned person is unclear. OFAC generally refuses to issue licenses for theoretical or potential scenarios or where US jurisdiction is uncertain. Perhaps OFAC would be willing to issue a license under a more uncertain set of facts when involving ransomware attacks, but this is not stated in the advisory.

4. Entities Facilitating Ransomware Payments Could be Money Transmitters Subject to FinCEN Registration and AML Compliance Requirements

FinCEN’s advisory notes that a number of third-party service providers, including digital forensics companies, cyber security firms, and insurance companies, often assist victims in making payments of cryptocurrency to attackers. According to FinCEN, “Depending on the particular facts and circumstances, this activity could constitute money transmission.” Money transmitters acting in whole or in substantial part in the United States are considered a money services business (MSB), which is a type of US financial institution subject to AML regulations promulgated by FinCEN. Among other requirements, MSBs must register with FinCEN, adopt a written AML compliance program with adequate policies and procedures, designate a chief compliance officer, provide training to appropriate personnel, and subject the compliance program to independent testing. MSBs are also required to implement internal controls to assess risks and file suspicious activity reports (SARs) with FinCEN for transactions it believes may involve suspicious conduct, potentially including ransomware-related payments.

5. FinCEN Publishes Red Flags for Financial Institutions

FinCEN’s advisory contains a list of 10 “red flag indicators” to “assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with ransomware attacks.” For example, red flag 5 describes a situation in which a financial institution’s customer “receives funds from a customer company and shortly after receipt of funds sends equivalent amounts to a [cryptocurrency] exchange.” Red flag 4 states, “A transaction occurs between an organization, especially an organization from a sector at high risk for targeting by ransomware (e.g., government, financial, educational, healthcare), and [a digital forensics and incident response company or a cyber insurance company], especially one known to facilitate ransomware payments.” Therefore, US financial institutions subject to AML compliance program requirements, including but not limited to MSBs, should consider whether these red flag indicators exist when deciding whether or not to file a SAR about a transfer. As a result, victims should understand that a service provider may submit a SAR to FinCEN, even if a ransomware payment is processed and not blocked or reported to OFAC.

Concluding Observations

Both OFAC’s and FinCEN’s guidance may make financial institutions, including banks and MSBs, such as payment processors and cryptocurrency exchanges, reluctant or unwilling to handle payments related to ransomware and, potentially, unwilling to provide financial services to companies involved in assisting ransomware victims. Victims of ransomware may be paralyzed in how to address these situations if there is some red flag indicator of a potential sanctions or money laundering risk and, potentially, even in the absence of a red flag given the strict liability approach to sanctions enforcement. As OFAC designates individuals and entities responsible for ransomware or other forms of cyber-related attacks, those victims threatened by ransomware need to be attentive of the risks. In addition, payments to ransomware attackers located in comprehensively-sanctioned countries present significant risks to US persons, and potentially non-US persons.
A premium will be placed on conducting as much due diligence as possible, documenting those efforts, and contacting OFAC, FinCEN, and other US law enforcement as appropriate. It is also possible that an emergency authorization from OFAC could be pursued.

From a broader policy perspective, it may be useful for OFAC to set up a special unit to handle such requests from ransomware victims in an expedited manner, and without a presumption of denial given the severe consequences of refusing ransom demands. The application of strict liability in enforcement actions involving activity that can often be conducted in an anonymous or pseudonymous manner may not be appropriate and OFAC could consider adopting an "actual knowledge" standard in these circumstances. OFAC could also consider crafting an appropriate general license with a reporting obligation, which would serve OFAC's interest in receiving potentially helpful information for the administration of its sanctions programs. Given the truly "between a rock and a hard place" situation in which ransomware victims and those assisting them find themselves, some rethinking of this aspect of US sanctions programs may be warranted. Similarly, FinCEN could consider issuing guidance that it will not penalize financial institutions that process transactions on behalf of ransomware victims so long as the financial institution makes a timely report to FinCEN and/or law enforcement regarding the transaction.

[1] On May 17, 2019, the European Union (EU) adopted new legislation for imposing sanctions on persons engaged in cyber-attacks on the EU, its member states or allies to the EU, effecting a long-standing initiative and continuing a series of policy and regulatory decisions by various governments—most notably the United States. Similar to the US sanctions regime, sanctioned individuals and entities are subject to asset freezes on all funds and economic resources that either belong to them or are owned, held or controlled by them.

The sanctions can be imposed upon occurrence of significant cyber-attacks that pose an external threat to the EU and its member states. “Significance” is determined by a range of factors, such as the scope, scale, impact or severity of disruption caused and the amount of data loss or economic loss. “External” means the attack is carried out, or supported, from outside the EU.

Sanctions can be imposed on individuals or entities who: (i) are responsible for cyber-attacks or attempted cyber-attacks, (ii) provide financial, technical or material support for or are otherwise involved in cyber-attacks or attempted cyber-attacks, including by planning, preparing, participating in, directing, assisting or encouraging these attacks or facilitating them whether by action or omission; or (iii) are associated with the entities or individuals covered under (i) and (ii). Similar to the US, making funds or economic resources available directly or indirectly to sanctioned individuals or companies or for their benefit is prohibited, leading to similar dilemma between paying or facilitating the payment of a ransom versus potential violating of sanction regimes. Contrary to the US though, the EU sanctions regime does not contemplate license applications, nor has it encouraged self-initiating a dialogue with law enforcement authorities.

The EU sanctions regime was extended in May 2020 until May 2021. It was first applied in July 2020, with Russian and Chinese companies and individuals being added to the sanctions list due to their (alleged) involvement in various cyber-attacks, such as the attempted cyber attack against the Organization for the Prohibition of Chemical Weapons and those publicly known as ‘WannaCry’, ‘NotPetya’, and ‘Operation Cloud Hopper’.

Practices
Privacy & Cybersecurity
Retail & E-Commerce
Export Controls
Economic Sanctions
Anti-Money Laundering

© 2021 STEPTOE & JOHNSON LLP. ALL RIGHTS RESERVED. ATTORNEY ADVERTISING.