CLIENT ALERTS & INSIGHTS

Ransomware Response Complicated by Growing Number of Sanctions in Wake of Russian invasion of Ukraine

APRIL 26, 2022

Authors: Ryan T. Sulkin

Entities facing significant legal risk, no matter the circumstances, if they make ransom payments to attackers connected to, or originating from Russia.

As the Russian invasion of Ukraine continues, the U.S. government continues to implement a multitude of sanctions against Russian individuals, banks, organizations, and entities.

A rise in cybercrime and cyber-attacks has also followed, with many emanating from Russia-linked hacking groups. These attacks include ransomware attacks. However, with the new sanctions in place, ransomware payments to groups linked to Russia are increasingly ill-advised. A recent example of U.S. sanctions against Russia entangling with ransomware attacks is the recent Treasury Department sanctions against the Russian-based Hydra Market and Garantex, both of which have been linked to a number of recent ransomware attacks.

The Treasury Department's Financial Crimes Enforcement Network ("**FinCen**") also recently sent out notices and guidance related to sanction evasion techniques. Some of the techniques flagged include use of cryptocurrency, Russian sponsored or linked ransomware techniques, or both.

Even the act of paying a ransom related to a ransomware attack is becoming more and more scrutinized, whether related to the Russia sanctions or not. For example, North Carolina became the first state in the US to ban its state agencies and local governments from paying ransoms While the law only applies to public entities, it shows the general trend against paying out related ransoms.

Ransomware attacks often lead to demands from the nefarious actors for various amounts of money, usually in the form of cryptocurrency. It is important to note that the Office of Foreign Asset Control ("**OFAC**") has indicated that all sanctions extend to virtual and cryptocurrency as well. Meaning, the sanctions are applicable to ransomware payments even if the attacker is requesting cryptocurrency instead of traditional currency.

With the increasing prevalence of ransomware attacks emanating from Russia, and in light of the growing list of sanctions levied against Russian entities, banks, and individuals, it is increasingly likely that Russian ransomware attacks are connected sanctioned entities, banks, and individuals. Therefore, entities face more legal issues and risk in the face of a ransomware attack.

Ransomware and Russia Sanctions

There are three main scenarios that could arise related to ransomware attacks and the current Russian sanctions.

1. Specifically Listed on the Sanctions Lists

The first scenario arises where a ransomware attack originates from an attacker specifically listed on one of OFAC's sanctions lists. In this case, any payment would violate the sanctions and be subject to civil penalties as described below. However, criminal penalties only apply where the violation was willful-meaning the entity or individual who violated the sanctions needs to have some form of knowledge that the attacker was on the OFAC sanctions lists prior to making the payment.

2. Not Specifically List, But Possibly Connected with Someone on the Sanctions Lists

The second arises where an entity or individual has reason to believe, or suspects, that the attacker is sanctioned through OFAC, but where the attacker's stated identity does not specifically appear on the OFAC sanction lists. An example of this would be where the attack came from a hacking group that uses a pseudonym, but that public reporting indicates is controlled by a sanctioned entity or individual.

If, the attacker is connected to someone, or is, on the OFAC sanctions lists, any payment would violate the sanctions and be subject to civil penalties as described below. Criminal penalties require a showing of "willfulness." Here, willfulness is likely due to the fact there is suspicion or belief that the attacker was connected to someone, or was, on the sanctions lists.

If, despite the significant legal risk, an entity makes the ransom payment suspecting the attacker is sanctioned but it turns out the attacker is **not** subject to OFAC sanctions, the entity would not face civil or criminal penalties.

3. Unknown if Connected with Someone on the Sanctions Lists

The third scenario arises where an entity or individual has **no** reason to believe, or suspicion, that the attacker is sanctioned through OFAC, and where the attacker's stated identity does not specifically appear on the OFAC sanction lists.

In this case, determining whether any payment would violate the sanctions is difficult, if not impossible, to ascertain. However, significant legal risk remains because, as stated above, "knowledge" is **not** a requirement for civil penalties to apply. Therefore, if an entity or individual is wrong and the attacker is actually sanctioned by OFAC, they would be subject to civil penalties. Criminal penalties are unlikely to apply here because the entity or individual had no belief or suspicion that the attacker was sanctioned by OFAC.

Similar to the second scenario, if the attacker turns out to **not** be subject to OFAC sanctions, the entity would not be subject to civil or criminal penalties if it makes the ransom payments.

Penalties For Violating Sanctions

Sanctions are handed down and promulgated by OFAC. However, enforcement can come both from OFAC and the Department of Justice as violating the sanctions can lead to both criminal and civil penalties. The Department of Justice takes the lead on criminal enforcement and OFAC takes the

lead on civil enforcement. Both criminal and civil enforcement can occur simultaneously, and one does not preclude the other.

Criminal penalties for a single, "willful" violation of the sanctions can lead to fines up to $1,000,000 and/or up to 20 years in prison per violation. Therefore, the government must show some form of knowledge in the alleged defendant's actions in order to bring criminal penalties. Under the third scenario described above where an entity has no knowledge or reason to believe the attacker is sanctioned, the entity would be safe from criminal penalties. However, knowledge is not a defense to civil penalties.

Civil violations are considered strict liability offenses meaning the government does not need to show any sort of knowledge element or mental state of any kind, only that the actions conducted by the alleged defendant violated the sanctions. The civil penalties can lead to fines up to $330,947 (or 2x the amount of the transaction, whichever is greater) per violation whether willful or not.

However, on the civil side, the penalties vary based on the value of the transaction involved. The applicable maximum civil penalties are the following based on the value of the transaction: (1) $10,000 if the transaction is valued between $1,000 and $10,000; (2) $25,000 if the transaction is valued between $10,000 and $25,000; (3) $50,000 if the transaction is valued between $25,000 and $50,000; (4) $100,000 if the transaction is valued between $50,000 and $100,000; (5) $200,000 if the transaction is valued between $100,000 and $200,000; or (6) The maximum ($330,947) if the transaction is valued at $200,000 or more.

The civil penalties levied also depends on subjective factors as well. For example, voluntary self-disclosure (e.g., notifying OFAC of any possible violations) can mitigate how much a defendant owes in civil penalties.

OFAC also considers the following (possibly aggravating) factors, among others, in determining the civil penalties: (1) willful or reckless violation of law; (2) prior notice; (3) concealment; (4) management involvement; (5) awareness of conduct; (6) commercial sophistication; (7) size of operations; (8) volume of transactions; (9) remedial response; and (10) cooperation with OFAC.

Other Legal Claims and Issues

Additionally, other standard legal claims apply in the case of business's failing to adequately prepare for such ransomware attacks. For example, if a Board of Directors for a corporation is found to be negligent in failing to protect the business (e.g., failing to implement a reasonable security program) the individual members could be held personally liable. Similar claims were filed against SolarWinds in relation to the massive data breach that occurred in 2020. In that case, the cybersecurity attack resulted from a Trojan Horse.

The increasing amount of government issues alerts (as discussed above) related to ransomware attacks and as it relates to cryptocurrency and sanctions would make it more difficult for entities to claim they were not aware of the threat. Therefore, entities should be preparing and implementing measures to properly guard against the ever growing threat of cybersecurity attacks and ransomware attacks.

Finally, as it gets more difficult to determine the legality of ransomware payments to groups in Russia, insurance companies that would normally provide coverage or assistance for such payments

or attacks, become less likely to provide coverage because Insurance companies are unlikely to payout coverage if that coverage would violate sanctions. Therefore, a normal remediation route some companies take might be off the table due to the increase in sanctions against Russian banks, individuals, and businesses.

Looking Ahead

As the threat of Russian cyberattacks, and especially ransomware attacks, increases, entities need to be aware of the possible legal ramifications and limit avenues for remediating or mitigating the attack. Entities face increasing and significant legal risk of civil penalties whether or not they are actually aware, or have knowledge as to whether, the attacker is sanctioned or not. If a business pays out a ransom, and that attacker happens to be sanctioned, OFAC can impose civil penalties.

Properly preparing contingency plans and business continuity plans, as well as having data recovery and backup systems in place, are crucial steps in planning for cybersecurity threats.

As the guidance and nuances of ransomware response continue to take shape, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Ryan T. Sulkin at rsulkin@beneschlaw.com or 312.624.6398.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.