BLANKROME

Cybersecurity & Data Privacy

OCTOBER 14, 2020 • NO. 15

# The Treasury Department's Office of Foreign Assets Control Issues Advisory Warning to Victims of Ransomware Attacks

Ransomware demands have surged during the pandemic. Earlier this month, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued an advisory pertaining to the financial implications of succumbing to ransomware demands and paying money to foreign actors who are subject to U.S. sanctions. This recent OFAC guidance underscores the need for a disaster preparedness plan, as well as the need for victims of ransomware attacks to immediately engage counsel to ensure compliance with the law when responding to an attack of this nature.

## OVERVIEW OF RANSOMWARE ATTACKS

Ransomware is a form of malicious software ("malware") designed to block access to a computer system or data, often by encrypting data or programs on information technology ("IT") systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. In some cases, in addition to the attack, the perpetrators will also threaten to publish sensitive files belonging to the victims or their customers. The consequences of a ransomware attack can be severe and far-reaching, with the potential to cause significant losses of sensitive, proprietary, and critical information and/or loss of business functionality.

Ransomware attacks can impact any business. Given the ongoing pandemic, businesses are relying on IT systems to maintain their daily operations now more than ever. The need for disaster preparedness plans is essential. Any disaster preparedness plan should include responding to a full-blown cyberattack like a ransomware demand, which oftentimes shuts down all of the business' IT infrastructure with no notice.

The Federal Bureau of Investigation ("FBI") has reported a 37 percent annual increase in disclosed ransomware cases between 2018 and 2019, and a 147 percent annual increase in associated losses over the same time period. Although the FBI has not released statistics for 2020, it is widely believed that these figures have increased by even larger margins over the course of the last year. Being ready to respond to a ransomware attack is critical.

## OFAC ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS

Earlier this month, OFAC issued an advisory that addresses some of the compliance issues that arise with ransomware. OFAC's guidance warns companies of the potential risk of violating U.S. sanction laws for making ransomware payments to individuals who are subject to U.S. sanctions.

The OFAC alert, which can be found here, reminds companies that the ransom payments, even if made under duress, are still covered by its sanctions regulations, which restrict dealings with certain targeted countries, regions, entities, and persons on grounds such as foreign policy, national security, and combatting weapons proliferation, transnational crime, narcotrafficking, and human rights abuses.

OFAC's sanctions regime prohibits payments to or transactions with specific persons or entities on OFAC's Specially Designated Nationals and Blocked Persons List ("SDN List"), and to certain embargoed countries and regions (*e.g.,* Cuba, Crimea, Iran, North Korea, and Syria) without securing a license. The alert identifies foreign actors in North Korea and Russia who have been recently added to the SDN List because of their involvement with ransomware and other types of malware attacks.

Importantly, the advisory further states that OFAC may impose sanctions "even if [the victim] did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanction laws and regulations administered by OFAC." While most OFAC trade sanctions restrictions apply on a strict liability basis, the alert stresses the importance of disclosure and cooperation with authorities as a key factor in mitigating any potential penalty exposure.

Many companies with an international footprint already have an OFAC compliance program. However, many domestic companies that do not regularly conduct business overseas lack a robust compliance program. OFAC's sanctions regime also applies to foreign businesses that utilize U.S. commerce to transact business. All domestic businesses need to be mindful of these obligations. Likewise, foreign businesses, which are just as susceptible to ransomware attacks, need to be aware of their obligations to comply with U.S. sanction laws.

Any business, foreign or domestic, that wishes to send money to someone on the SDN List must obtain a license from OFAC if it involves U.S. commerce. The advisory reiterates the broad reach of U.S. sanction laws:

> Additionally, any transaction that causes a violation…, including transactions by a non-U.S. person which causes a U.S. person to violate any…sanctions, is also prohibited. U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons, which could not be directly performed by U.S. persons due to U.S. sanctions regulations.

By way of example, V, a foreign company, decides to pay a ransomware payment to company in Iran. That company does not seek a license from OFAC, and instead wires U.S. dollar-denominated funds from its foreign bank account to purchase cryptocurrency to pay the ransom demand. That payment (like most U.S. dollar transactions) clears through a U.S. correspondent bank. As a result, that transaction would violate the OFAC sanction regime and could subject V to a burdensome investigation and potential penalties under U.S. sanctions laws. Worse, if such a transaction was undertaken knowingly or with an intent to evade the sanctions, V also could run afoul of U.S. money laundering, bank, and wire fraud statutes.

## CONCLUSION

Paying a ransomware demand is generally discouraged. However, in some instances companies may make the business decision to meet the financial demands of cyber criminals in order to maintain continuity of operations or protect confidential information from being widely disseminated. OFAC's advisory creates an added layer of complexity and underscores the vital need to prepare for a ransomware attack. The sensitive compliance issues set out in the advisory highlight the benefits of working with experienced counsel, who can guide victims of ransomware in navigating the crisis while ensuring that any actions taken in response do not violate federal law.

**For additional information, please contact:**

**David J. Oberly, Cincinnati Office | Associate, Cybersecurity & Data Privacy | 513.362.8711 | doberly@blankrome.com**
**Jed M. Silversmith, Philadelphia Office | Of Counsel, White Collar Defense & Investigations | 215.569.5789 | jsilversmith@blankrome.com**
**Matthew J. Thomas, Washington, D.C. Office | Partner, International Trade | 202.772.5971 | mthomas@blankrome.com**