faegre drinker

October 06, 2020

Ransomware Payments May Violate Sanctions Laws, U.S. Treasury Department Warns

On October 1, 2020, the United States Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an advisory to companies that pay a ransom in the wake of a cyberattack. Specifically, the advisory warned that ransomware attack victims and third-parties who assist these victims could be in violation of federal law if they pay or facilitate the payment of a ransom to a sanctioned individual or entity — intentionally or otherwise. In light of dramatic increases in both the frequency and severity of ransomware attacks during the COVID-19 pandemic, companies should closely review the OFAC advisory and ensure that they take appropriate steps to avoid violating the U.S. sanctions laws if they are victimized by a ransomware attack.

Under the International Emergency Economic Powers Act (IEEPA) and the Trading with the Enemy Act (TWEA), among other laws, executive orders, and regulations, U.S. persons generally are prohibited from engaging in transactions — directly or indirectly — with individuals or entities "designated" on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), as well as persons or entities covered by comprehensive country embargoes (e.g., Cuba, Iran, North Korea, Syria, and the Crimea region of Ukraine). These sanctions also apply to entities owned 50% or more by persons on the SDN List.

Pursuant to various sanctions programs, OFAC previously placed numerous malicious cyber actors on the SDN List. These designated actors include perpetrators and facilitators of ransomware attacks. For example, in September 2019, OFAC designated the Lazarus Group, a cybercriminal organization sponsored by North Korea, after the group launched the May 2017 ransomware attack known as WannaCry 2.0. And in December 2019, OFAC designated the Russia-based Evil Corp and its leader, Maksim Yakubets, for their development and distribution of the Dridex malware.

Individuals and entities who willfully initiate or facilitate a financial transaction with a SDN or a comprehensively

embargoed jurisdiction may face significant criminal penalties, including up to 20 years in prison for individuals and fines of up to $1 million. As noted above, the OFAC advisory conspicuously notes that civil penalties may be imposed for sanctions violations even if the parties who initiate or facilitate the transaction did not know or have reason to know that they were engaging in a prohibited transaction — in other words, based on strict liability.

The OFAC advisory encourages ransomware victims to self-report attacks and ransom payments to law enforcement. In determining the "appropriate enforcement outcome" for a ransomware payment made to a sanctioned individual or entity, OFAC will consider the victim's "self-initiated, timely, and complete report of a ransomware attack to law enforcement" and "[f]ull and timely cooperation with law enforcement" as significant mitigating factors. The advisory further "encourages" companies to install an appropriately-tailored, risk-based compliance program that mitigates the risk that a ransomware payment will have to be made and, if made, the consequence of making payment to a SDN or comprehensively embargoed jurisdiction.

In conjunction with OFAC's advisory, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) issued a separate advisory to companies that facilitate ransomware payments, instructing them to consider filing a Suspicious Activity Report (SAR) when dealing with a ransomware demand.

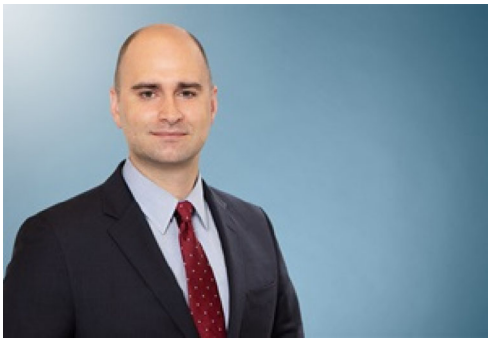
These new advisories are certain to influence how victims and third-party advisers respond to ransomware attacks. While attacks had grown in frequency and severity prior to COVID-19, ransomware activity has dramatically increased during the pandemic, particularly for U.S.-based victims. In the past, many victims elected to pay ransoms in order to quickly regain access to their data and resume normal business operations. However, the new guidance from OFAC and FinCEN will force victims and their advisers to seriously consider the risk that a ransom payment might violate U.S. sanctions laws and result in significant criminal or civil liability. Ultimately, the decision about whether to pay a ransom will involve balancing many factors, including the significance of the affected data and the relative risk that the attacker is a sanctioned individual or entity.

To minimize the risk of violating U.S. sanctions laws in connection with responding to a ransomware attack, companies should consider these action items:

- **Update and Secure Backups** — The only way to ensure a ransom payment is not made to a sanctioned individual or entity is to not pay a ransom at all. The best way to avoid paying a ransom is to ensure that your business has data backups that are both up-to-date and secure. To ensure adequate security, businesses should maintain their backups separately from networks — either offline or through a separate cloud-based service. Businesses also should consider using other safety measures, like multi-factor authentication and separate administrative credentials. Companies should also regularly test their backups and record the time it takes to restore vital systems.

- **Perform Due Diligence** — Before initiating a ransom payment, the victim and any third-party advisers should conduct reasonable due diligence on the malicious actors. This due diligence should be completely and accurately documented. Reasonable due diligence should include a search of OFAC's SDN List — which now includes crypto wallet addresses for designated individuals and entities. Efforts also should be made to determine whether the attackers are affiliated or associated with a comprehensively embargoed jurisdiction — for example, by researching malware variants and email domain(s) associated with the malicious actors to determine if they are associated with embargoed countries.
- **Notify and Cooperate with Law Enforcement** — Whenever making a ransomware payment, victims and their advisers should consider alerting the Federal Bureau of Investigation (FBI) — through either the FBI's Internet Crime Complaint Center or the local FBI field office. Victims should be prepared to provide law enforcement with an overview of the attack, any identifying information about the attackers and their crypto-currency accounts, and information about the ransom demand itself. If a ransom payment is ultimately determined to have been paid to a sanctioned individual or entity, voluntary disclosure to law enforcement and OFAC should be evaluated and strongly considered. OFAC will view the victim's prior cooperation with law enforcement to be a significant mitigating factor.
- **Institute an Appropriate Risk-Based Compliance Program** — The OFAC advisory encourages companies to customize their compliance and security programs based on their unique business risk profile. OFAC has previously issued a framework for compliance that "strongly encourage[d]" companies to incorporate five "essential components" of compliance: management commitment, risk assessment, internal controls, testing and auditing, and training. Companies should assess and update their risk-based compliance program regularly to ensure that they can respond to pernicious and ever-evolving ransomware threats.

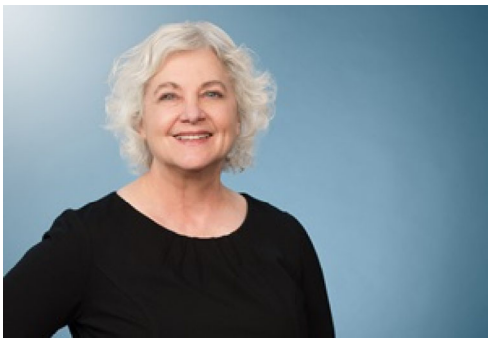
MEET THE AUTHORS



Peter W. Baldwin

Partner

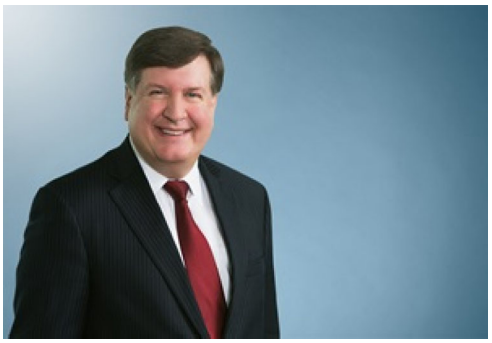
+1 212 248 3147
New York
peter.baldwin@faegredrinker.com



M. Angella Castille

Partner

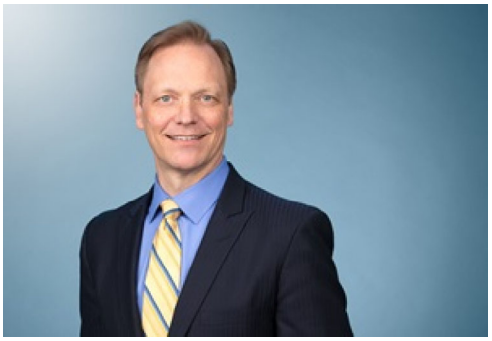
+1 202 589 2849
Washington, D.C.
angella.castille@faegredrinker.com



Kenneth K. Dort

Partner

+1 312 569 1458
Chicago
kenneth.dort@faegredrinker.com



Paul H. Luehr

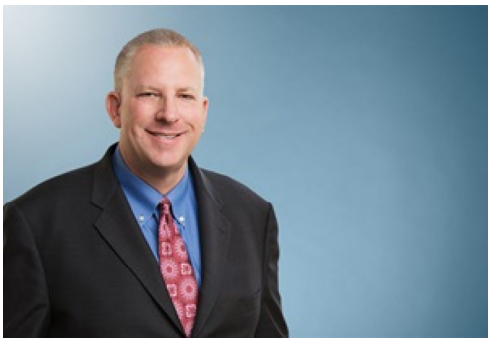
Partner

+1 612 766 7195
Minneapolis
paul.luehr@faegredrinker.com

Adam W. Smith

Associate

+1 612 766 8762
Minneapolis
adam.smith@faegredrinker.com



Jason G. Weiss

Counsel

+1 310 203 4062
Los Angeles
jason.weiss@faegredrinker.com

Services and Industries

Government & Regulatory Affairs

Privacy, Cybersecurity & Data Strategy

Litigation