International Trade Update

September 2021

Treasury Department Issues Updated Advisory on Ransomware Payments

Ransomware attacks have been increasing, forcing many businesses to choose between paying a ransom and losing access to their confidential and proprietary data or information networks and systems. On September 21, the Department of the Treasury issued an updated advisory that highlights potential sanctions risks for companies that directly make or otherwise facilitate ransomware payments and offers "proactive steps" companies can take to mitigate such risks. The advisory updates guidance offered in October 2020, which highlighted that anti-money laundering and economic sanctions regulations implemented and enforced by Treasury's Office of Terrorism and Financial Intelligence may be triggered by persons or companies involved in facilitating ransomware payments. In turn, organizations should consider this advisory, as well as other federal resources and guidance, when updating their data breach response plans and compliance programs.

Background: The Advisory

Ransomware attacks are increasing in size, sophistication and frequency. According to the FBI, there was "a nearly 21 percent increase in reported ransomware cases and a 225 percent increase in associated losses from 2019 to 2020." In 2020 alone, ransomware payments totaled over $400 million. The financial harm caused by these attacks, however, is not limited to these payments, as the economic damage extends to the disruption of critical sectors, including financial services, health care and energy, as well as the exposure of confidential corporate and personal information.

The Treasury Department's advisory notes that companies "that facilitate ransomware payments to cyber actors on behalf of victims, including 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." Since 2013, Treasury's Office of Foreign Assets Control (OFAC) has designated numerous malicious cyber actors under its cyber-related sanctions program. The advisory notes that OFAC will continue to impose sanctions on such actors "and others who materially assist, sponsor, or provide financial, material, or technological support for these activities," as such support "may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims." The U.S. government discourages payment of any cyber ransom, as such payment may be to sanctioned persons or to comprehensively sanctioned jurisdictions where the funds could be used for activities adverse to U.S. national security.

Virtual Currency Exchanges

The Treasury Department indicates that virtual currency exchanges are a critical element and the principal means of facilitating ransomware payments and associated money laundering activities. While most virtual currency activity is commercial and lawful, the process can be used for illicit activity through peer-to-peer exchangers, mixers and exchanges, including facilitating sanctions evasion, ransomware schemes and other cybercrimes. In conjunction with releasing Treasury's updated advisory, OFAC announced the designation of virtual currency exchange SUEX OTC, S.R.O. (SUEX) for its part in facilitating financial transactions for certain malign ransomware actors. According to OFAC, SUEX has facilitated transactions involving illicit proceeds from at least eight cyberattacks and the resulting ransomware payments.

This is the first OFAC sanctions designation against a virtual currency exchange and, as a result, SUEX has been added to the Specially Designated Nationals List. As of September 21,

all property and interests in property of SUEX that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, 50% or more by SUEX are also blocked. U.S. persons are generally prohibited from engaging in transactions with SUEX absent a specific license from OFAC.

Enforcement Actions and Mitigating Risk

The Treasury Department's advisory reminds organizations that enforcement actions for violations of the federal government's sanctions programs can range from non-public responses (e.g., No Action Letter or Cautionary Letter) to public responses (e.g., civil monetary penalties) and states that non-public responses are more likely when impacted parties undertake certain "mitigating steps," such as reporting ransomware attacks to, and cooperating with, law enforcement. Although a comprehensive and effective sanctions compliance program is an important tool for mitigating exposure to sanctions-related violations, the advisory focuses on information sharing as another key aspect of mitigating risk. More specifically, the advisory references the Cybersecurity and Infrastructure Security Agency (CISA), FBI field offices, FBI Internet Crime Complaint Center and local U.S. Secret Service offices as the federal agencies and offices that organizations should engage and cooperate and share information with following a ransomware attack.

However, organizations should consider whether they can disclose data breach reports and other internal information to federal agencies in a manner that preserves certain privileges and protections. For instance, according to the Cybersecurity Information Sharing Act of 2015, providing cyber threat indicators and defensive measures to the federal government pursuant to certain federal information sharing programs will not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection. Accordingly, organizations should familiarize themselves with the federal government's information sharing programs and build the most appropriate ones into their data breach response plans so they are better prepared to engage in such activities following a ransomware attack or other security event.

Security Measures and Other Resources

The Treasury Department's advisory notes that organizations should adopt comprehensive information security measures and controls, such as those set forth in CISA's September 2020 Ransomware Guide. It also recommends that organizations implement security practices to better protect their information technology networks and systems, including:

- Maintain offline data backups
- Develop incident response plans
- Institute cybersecurity training
- Regularly update antivirus and anti-malware software
- Employ authentication protocols

Interestingly, the advisory comes only a few months after the White House published an open letter to corporate executives and business leaders urging them to take similar proactive measures to defend against the recent increase in ransomware attacks. The letter and the advisory each reference additional resources and guidance that organizations can use to build a comprehensive data breach response plan and international trade compliance program.

FOR MORE INFORMATION

For more information, please contact:

Francesca M.S. Guerrero
Partner, International Trade
202.973.2774
Francesca.Guerrero@ThompsonHine.com

Steven G. Stransky
Partner, Business Litigation
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com

Samir D. Varma
Partner, International Trade
202.263.4136
Samir.Varma@ThompsonHine.com

Scott E. Diamond*
Senior Legislative & Regulatory Policy Advisor, International Trade
202.263.4197
Scott.Diamond@ThompsonHine.com

**Not licensed to practice law*