Alert

October 8, 2020

COZEN O'CONNOR

Happy Cybersecurity Awareness Month: OFAC and FinCEN Issue New Advisories on Ransomware Payments

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN) kicked off National Cybersecurity Awareness Month with a pair of advisories relating to ransomware attacks. On October 1, 2020, OFAC and FinCEN issued "Potential Sanctions Risks for Facilitating Ransomware Payments" and "Ransomware and the Use of the Financial System to Facilitate Ransom Payments" respectively.

OFAC

The OFAC advisory reminds companies of the potential sanctions exposure arising from payments or the facilitation of payments made in response to ransomware attacks. Specifically, the advisory gives notice that companies that pay or facilitate ransom could violate sanctions regulations if payments are being made to sanctioned countries or persons, such as individuals or entities on the Specially Designated Nationals and Blocked Persons List (SDN list). Thus, ransomware victims could be subjected, not only to the potential loss of critical data or the expense of having that data restored, but to the added insult of being assessed penalties for engaging in transactions with sanctioned parties.

OFAC notes that ransomware attacks have been increasing in frequency and sophistication over the past few years, and particularly this year, as companies have moved more of their business online during the COVID-19 pandemic. Moreover, investigative agencies have identified several criminal actors conducting ransomware attacks as having ties to or residing in countries such as North Korea, Iran, and Russia. Thus, there may be national security implications where ransomware payments to such bad actors may be used to fund objectives adverse to U.S. national interests. OFAC further cautions that payments made by victims embolden criminal actors and that, ultimately, ransom payments offer no guarantee of released files or information.

Ransomware victims are encouraged to immediately contact law enforcement and other relevant agencies, such as the Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection. In addition, a company that is subject to a ransomware attack is advised to immediately notify OFAC if it believes a ransomware payment may implicate OFAC sanctions. Unfortunately, the agency also advises that, due to the national security implications, applications for licenses to pay ransom to sanctioned countries or persons will be reviewed on a case-by-case basis with a presumption of denial.

Despite this somewhat gloomy outlook, OFAC states that it will consider the timeliness of notice and willingness to cooperate with authorities as a significant mitigating factor "in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus." This at least suggests a realization by OFAC that many companies may feel that they have no choice but to pay their captors.

FinCEN

FinCEN's companion advisory is mainly directed to companies that provide protection and mitigation services to victims of ransomware attacks including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response.

The FinCEN advisory identifies trends and attributes of ransomware activity and associated payments. Unsurprisingly, it also echoes OFAC's prognosis for increased ransomware attacks. FinCEN also describes some of the tactics being used by cybercriminals and identifies 10 "Financial Red Flag Indicators of Ransomware and Associated Payments." Ultimately, the FinCEN

Kathryn Sobotta

Associate

ksobotta@cozen.com
Phone: (202) 463-2528
Fax: (202) 861-1905

Related Practice Areas

- Technology, Privacy & Data Security
- Trade Regulation, Export Controls & Sanctions
- Transportation & Trade

advisory is a reminder to financial institutions of their obligations under the Bank Secrecy Act and their responsibility to file suspicious activity reports when they have reason to believe that a transaction relates to illegal activity.

While it does not appear that any penalties have thus far been assessed by OFAC with regard to ransomware payments, the tone and timing of these advisories suggest an increased threat level and increased regulatory scrutiny. Businesses hit with a ransomware attack may feel they are in a catch-22 situation where they must choose between restoring their data or complying with sanctions regulations. Unfortunately, there is no easy answer. However, taking a proactive approach might ease the pain. In addition to deploying robust cybersecurity protections to lessen the risk of an attack, companies are encouraged to develop ransomware response policies and training programs. These will at least provide employees with a roadmap and an understanding of their options before an attack happens.