The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2020
PHILADELPHIA, MONDAY, NOVEMBER 2, 2020 VOL 262 • NO. 87 An ALM Publication

CYBERLAW

Between a Rock and a Hard Place: Advisories Target Ransomware Victims, Insurers

BY JOSHUA A. MOONEY AND LINDA D. PERKINS
Special to the Legal

Between a rock and a hard place—a very bad Rolling Stones song, and a place ransomware victims and their insurers may be finding themselves in soon. On Oct. 1, the Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC) in the U.S. Department of the Treasury collectively issued a pair of advisories warning ransomware victims, their insurers, and their incident response teams of potential sanctions for facilitating a ransomware payment.

The FinCEN Advisory identifies which corporate officers and employees should receive the advisory, effectively placing those individuals on notice as to their responsibility for an organization's "sanctions compliance program." The OFAC Advisory warns against "engaging in transactions, directly or indirectly, with individuals or entities ('persons') on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes."


MOONEY


PERKINS

JOSHUA A. MOONEY *is a partner at White and Williams where he serves as chair of the firm's cyber law and data protection group.*

LINDA D. PERKINS *is counsel at the firm. She focuses her practice on cybersecurity and privacy laws.*

What should victim organizations do? Microsoft's Digital Defense Report for instance, concluded that threat actors have rapidly increased in sophistication between October 2019 and July 2020. The COVID-19 pandemic and resulting need for organizations to transform from onsite to remote workforces overnight have placed even greater strain on cybersecurity defenses. There are no hard answers for organizations, or for their insurance carriers for that matter. That can be frustrating. However, the advisories offer measures that companies may implement in their compliance programs and response procedures, and suggest that insurers may need to further emphasize pre-incident

The advisories offer measures that companies may implement in their compliance programs and response procedures, and suggest that insurers may need to further emphasize pre-incident preventative measures to mitigate potential liability.

preventative measures to mitigate potential liability.

RANSOM PAYMENTS AND THE ADVISORIES

Ransomware attacks have increased in sophistication, severity and frequency. They are carried out against large corporations, midsized companies, and small organizations, as well as against government agencies, hospitals, universities and school districts. Further, the past year has seen a dramatic rise of "double extortion schemes" in which attacks exfiltrate sensitive data before encrypting data on the target's information systems. The attackers then threaten to publish or sell the stolen data if the victim does not pay the demanded ransom.

Processing ransomware payments is a multi-step process involving at least one depository institution and one or more money services businesses (MSBs). The victim obtains convertible virtual currency (CVC) from a CVC exchange and transmits the payment, often from a wallet hosted by the exchange, to the cybercriminal's designated account or CVC address. The criminal then launders the funds through various means, including mixers and tumblers to convert the payment into other CVCs and smurfing transactions, across multiple accounts and exchanges to avoid tracing and detection.

In its advisory, FinCEN concludes that digital forensics and incident response firms, as well as cyber insurers, that assist victims to effect ransom payments may be subject to the Bank Secrecy Act and thus are required to file a suspicious activity report (SAR) with FinCEN upon any such payment. Specifically, FinCEN reasons that assisting ransomware victims, whether by providing funds or assisting with the exchange and transmission of CVC payments, can constitute a "money transmission." By engaging in "money transmission" activities, the advisory states, such organizations are required to register with FinCEN as a MSB and are subject to Bank Secrecy Act requirements, including the filing of SARs. The advisory states that SARS must include "all relevant information available, including cyber-related information." The advisory further warns that "persons involved in ransomware payments must also be aware of any OFAC-related obligations that may arise from that activity."

In its own advisory, OFAC threatens that ransom payments made to OFAC-designated organizations, some of whom, like Evil Corp and the Lazarus Group (which are well known for their ransomware exploits) can result in sanctions. The advisory explains that U.S. citizens, wherever located, are prohibited from "engaging in transactions, directly or indirectly, with individuals or entities (persons)" designated by OFAC as malicious cyber actors and that ransom payments can violate this prohibition. The advisory thus concludes:

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.

OFAC's reasoning: OFAC sanctions persons and organizations that "assist, sponsor, or provide financial, material, or technological support for" ransomware attacks. OFAC views the payment of ransoms within the scope of these prohibited activities. OFAC, moreover, may impose civil penalties based on strict liability—meaning that "a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC."

Thus together, FinCEN advises cyber insurers and response firms to register as MSBs and to file a detailed SAR each time they assist with a ransomware payment. OFAC advises that making or assisting with such payments may violate U.S. law and trigger civil fines under strict liability. When faced with the alternative—that a ransomware victim not pay and shut its doors, or that a cyber insurer deviate from the terms of a policy, it's not unreasonable to conclude that the advisories create a Catch-22.

MODIFYING (OR IMPLEMENTING) A SANCTIONS COMPLIANCE PROGRAM

Implementing or modifying a data security program to account

for these advisories can help mitigate both ransomware risk and liability exposure suggested in each advisory. To that end, OFAC has issued "A Framework for OFAC Compliance Commitments" to convey "the five essential components" of a sanctions compliance program (SCP). Those components are: a commitment from the organization's management to support the SCP in terms of resources, legitimacy, and culture; periodic risk assessments to create a risk-based design and updates of the SCP; internal controls, including policies and procedures, to identify, escalate, report (as appropriate), and record activity that may be prohibited by laws and regulations administered by OFAC; auditing and testing to assess the effectiveness of current processes and check for inconsistencies between these and day-to-day operations; and training of all appropriate employees and personnel to provide job-specific knowledge; communicate SCP responsibilities; and hold employees accountable for SCP training.

In other contexts, OFAC has considered the implementation or absence of internal measures when assessing fines. For instance, in a 2020 Finding of Violation, OFAC concluded that several mitigating factors weighed in favor of not imposing a monetary penalty, including the facts that the company had modified its internal controls to prevent reoccurrence of the violation, and that the company had cooperated with OFAC's investigation, which included voluntary disclosure to OFAC. In the context of ransomware attacks, OFAC's Enforcement Guidelines consider a company's "self-initiated, timely, and complete report of a ransomware attack to law enforcement" as a "significant mitigating factor" in determining an appropriate enforcement outcome, including monetary liability, if the situation is later determined to be sanctionable. The guidelines also state that OFAC will consider a company's "full and timely cooperation with law enforcement both during and after a ransomware attack" to be a "significant mitigating factor" for assessing sanctions. Thus, companies should continue to design and implement effective measures to mitigate against the risk of ransomware to strengthen their programs, and modify measures taken when responding to ransomware attacks. Companies should begin this process now.

OFAC also suggests that it may approve or "license" certain ransomware payments. The advisory states that "ransomware payments benefit illicit actors and can undermine the national security and foreign policy objectives of the United States," thus "license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial." OFAC also "encourages" victims "and those involved with addressing ransomware attacks" to notify OFAC "immediately" if they believe a requested ransomware payment would be sanctionable. Thus, reviewing OFAC's designation lists, as well as considerations of notifying OFAC of a ransomware attack, should be implemented into response procedures and discussed during table-top exercises.

What does all this mean? Presumably unable to effect a coordinated and effective response to the explosion of ransomware, FinCEN and OFAC are turning their attention to victims who make ransomware payments. Further development in this area will depend on what actions FinCEN and OFAC take or don't take. In the meantime, companies, incident response firms, and cyber insurers alike should consider these advisories and the potential need to undertake additional safeguards and procedural steps when responding to a ransomware attack. Insurers should understand the risks. The need for effective preventative measures may never be greater. •