OFAC's Ransomware Advisory Part 2 – How Banks Can Reduce Their Sanctions Risk for Client Cyber Ransom Payments

October 5, 2021

On September 21, 2021, the U.S. Department of the Treasury's Office of Foreign Asset Control ("OFAC") released an updated advisory (the "Advisory") on the sanctions risks associated with facilitating ransomware payments. The Advisory applies to victims of ransomware attacks, as well as companies that facilitate payments to threat actors, including financial institutions. In Part 1, we discussed the Advisory generally, and ways that victim companies can reduce their sanctions risks. In this Part 2, we discuss the measures that financial institutions can adopt to mitigate their ransomware sanctions risks, and why those compliance controls differ from the steps being taken by victims.

As we noted in Part 1, sanctions risks associated with ransomware payments are significant because of the strict liability nature of civil OFAC penalties and the increased difficulty of accurately identifying who exactly is receiving the payment. Threat actors that have been sanctioned often disband and reappear with new names and updated tools, and many non-sanctioned threat actors have been using ransomware tools developed by sanctioned threat actors or are otherwise partnering with sanctioned entities in their attacks.

Recognizing the risk, the Advisory provides that OFAC will consider a company's sanctions compliance program, as well as its collaboration with law enforcement, when deciding whether to issue a penalty, warning, or "no action" letter if a company has inadvertently made a ransomware payment to a sanctioned threat actor. But, in terms of compliance and diligence, financial institutions that facilitate ransomware payments on behalf of their clients are in a very different position than the victims of the attacks.

Different Role and Different Risks for Banks. In October 2020, the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") released an advisory that emphasized the critical role financial institutions play in cyber ransom payments and identified 10 red flags of ransomware-related illicit activity. But accurately identifying transactions that are associated with ransomware payments is difficult, and banks are almost always informed of their clients' ransomware incidents late in the process, after a decision has been made to pay (if they are informed of the incident at all). And even when a bank accurately flags a ransomware payment, or is told

by a client that a particular transaction is connected to a cyber ransom demand, the bank is rarely provided with any details. At that point, the client has likely made the determination that making a payment is essential for it to be able to restore operations, so any unnecessary delay in making the payment has the potential of causing the client significant economic damage. Under those circumstances, it is impractical for the bank to start conducting its own separate diligence or engaging directly with law enforcement (unless the client or law enforcement has requested that from the bank).

Accordingly, financial institutions should consider two different protocols for reducing ransomware sanctions risks, one protocol for when they are the victim of a ransomware attack, and another protocol for when they are facilitating payments on behalf of a client victim.

Measures Banks Should Consider to Mitigate Cyber Ransom Sanctions Risks. Although it is impractical for banks to be conducting independent comprehensive sanctions diligence for potential ransomware payments, financial institutions can reduce their sanctions risks by taking reasonable steps to identify transactions that are likely associated with ransomware payments and ensuring that their clients have conducted sufficient diligence before a payment is made. Consistent with our previous guidance on managing sanctions compliance risk generally, banks should consider adopting the following measures for potential ransomware payments by their clients:

- **Management Awareness**: Banks should consider briefing their senior leadership on these risks and updating them as to the measures that are being taken to reduce the risk, as well as any instances where significant compliance failures have been detected.

- **Risk Assessments**: Banks should consider designing reviews geared toward identifying clients, sectors, product lines, and geographies with historical or anticipated risk for ransomware payments. These reviews can help determine which areas of the bank's business may require heightened consideration for sanctions compliance.

- **Internal Controls**: OFAC guidance and enforcement actions make clear that having risk-based internal controls can significantly mitigate the potential for sanctions enforcement. For ransomware payments, banks should consider the following potential controls:

    - **Identifying Potential Ransom Payments**: Developing processes and procedures for identifying transactions that may be associated with cyber ransom payments. For example, creating automated alerts for large transfers to the major cyber ransom negotiators (the entities that most often make the actual cryptocurrency

payment to the threat actor) may help financial institutions identify potential cyber ransom payments. In a recent enforcement action, OFAC identified technology that can flag potentially sanctioned payments as a mitigating factor.

  - **Questions for Clients**: Creating a set of questions for clients associated with a transaction that may be connected with a cyber ransom payment that probe the extent of the client's due diligence. Those questions may include (i) the identity of the threat actors involved; (ii) the basis for the identification of the threat actors; and (iii) whether law enforcement has been consulted about the incident and the payment.

  - **Sanctions Check**: Conducting a sanctions check on the threat actors and associated crypto wallets that have been identified by the client.

  - **Client Certification**: Asking clients to sign a certification regarding the payment. Such certification may include the basis for the client's determination (i) as to the identity of the payment recipient, and (ii) that the payment is not being made to a sanctioned entity.

- **Testing Controls**: Consider establishing processes and procedures to test these controls and make improvements as appropriate.

- **Training**: Banks should consider offering training to employees who may encounter cyber ransom payments to help them identify, address, and escalate the associated sanctions risks.

- **Strong Cybersecurity**: In Part 1, we noted that OFAC will now be considering the sufficiency of a victim's cybersecurity program in deciding whether to bring an enforcement action relating to a ransomware payment, and offered some tips on data protection measures that can reduce risk. It is unclear from the Advisory, however, whether OFAC would also consider the cybersecurity measures of a bank that inadvertently facilitated a client's ransomware payment. That said, having a strong cybersecurity program will certainly be a mitigating factor when the bank itself was the victim making the payment, so that is worth considering as part of a risk mitigation program.

- **FinCEN Reporting**: Finally, financial institutions have reporting obligations that other entities in the ransomware payment lifecycle do not. As reiterated in the FinCEN advisory, banks must comply with their Bank Secrecy Act obligations by filing suspicious activity reports "when dealing with an incident of ransomware conducted *by, at, or through* the financial institution."

We will closely follow developments in this area and provide any updates at the Debevoise Data Blog.

To subscribe to our Data Blog, please click here.

* * *

Please do not hesitate to contact us with any questions.

The authors would like to thank summer associates Charlotte Blatt and Lexi Gaillard for their contributions to this blog post.

WASHINGTON D.C.

Luke Dembosky
ldembosky@debevoise.com

Satish M. Kini
smkini@debevoise.com

NEW YORK

Avi Gesser
agesser@debevoise.com

Scott M. Caravello
smcaravello @debevoise.com

SAN FRANCISCO

H Jacqueline Brehmer
hjbrehmer@debevoise.com