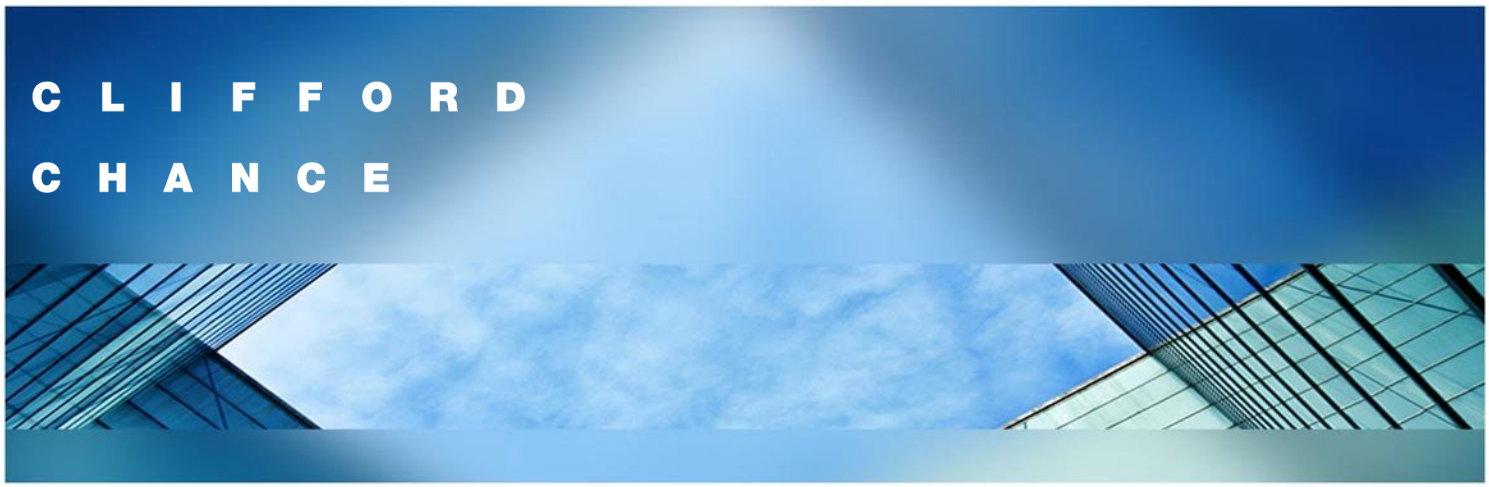

TREASURY RANSOMWARE ADVISORIES WARN COMPANIES TO CONSIDER COLLATERAL LEGAL RISKS IN PAYMENTS

On October 1, 2020, the US Department of Treasury issued a pair of advisories aimed at financial institutions and other corporates who may find themselves in the unfortunate position of being extorted to make payments to bad actors, or to process such payments, in connection with ransomware attacks. Both advisories remind companies in their crisis management considerations to consider the related money-laundering and sanctions risks. Companies should include these considerations in their ransomware playbook.

The Financial Crimes Enforcement Network ("FinCEN") advisory, "*Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*" ("FinCEN Advisory"),[1] and the Office of Foreign Assets Control ("OFAC") advisory, "*Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*" ("OFAC Advisory"),[2] both reinforce the responsibility of those dealing with such attacks to consider and comply with existing regulations. Neither the FinCEN Advisory nor the OFAC Advisory creates new obligations, but each contains important reminders regarding compliance risks and reporting requirements that companies who face ransomware attacks, or financial intermediaries who may process ransomware payments, cannot overlook.

The FinCEN Advisory highlights the role and obligations of financial institutions and other intermediaries, and provides guidance on ransomware typologies and red flags. FinCEN expects financial intermediaries to try to detect fund transfers that may be associated with ransomware attack demands and lists ten red flags that should be added to detection scenarios/algorithms. While the red flags are similar in some respects to those financial institutions should already be considering as part of general financial crime/money laundering detection, they focus specifically on certain types of third parties that often are involved in ransomware payments, such as digital forensics and incident response ("DFIR") companies and cyber insurance companies ("CICs"). The red flags further

1 https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.
2 https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

highlight the fact that the payments often involve convertible virtual currency ("CVC"). FinCEN provides the following examples:

- "a transaction occurs between an organization, especially an organization from a sector at high risk for targeting by ransomware (e.g., government, financial, educational, healthcare), and a DFIR or CIC, especially one known to facilitate ransomware payments"; and
- "a DFIR or CIC customer receives funds from a customer company and shortly after receipt of funds sends equivalent amounts to a CVC exchange."

The FinCEN Advisory also includes a request relating to Suspicious Activity Report ("SAR") filings, specifically, that financial institutions (i) reference "CYBER-FIN-2020-A006" in SAR field 2 (the field where financial institutions can include a note to FinCEN); (ii) select SAR field 42 (Cyber event) as the associated suspicious activity type, as well as select SAR field 42z (Cyber event - Other) and include “ransomware” as a keyword; and (iii) include any relevant technical cyber indicators related to the ransomware activity and associated transactions within the available structured cyber event indicator SAR fields 44(a)- (j), and (z).

The OFAC Advisory reminds companies, individuals, banks, and insurance companies subject to its broad jurisdiction and strict liability regime that one of the considerations, of many, when deciding to make a payment to a bad actor in a ransomware attack is whether the payment would create potential OFAC liability. Specifically, entities must consider whether the payment is to a Specially Designated National ("SDN") or otherwise implicates the OFAC sanction programs, including OFAC's country-wide sanctions. OFAC has listed as SDNs several entities found to be perpetrating these types of cyberattacks.

It is easy to see how in a moment of crisis a decision could be made to make a payment to save the company from imminent harm without necessarily conducting a sanctions risk review. However, the OFAC Advisory makes clear that enforcement consequences cannot be avoided simply because a payment was made under the duress of a ransomware attack. OFAC expects companies, including the victims of such attacks, to comply with its regulations, as would any financial institution processing any part of the payment. However, the OFAC Advisory does not provide any comfort that companies or financial institutions will be able to obtain an OFAC specific license for a ransomware payment even if they identify a sanctions risk because license applications involving ransomware payments "as a result of malicious cyber-enabled activities" are subject to a presumption of denial.

However, in the event an OFAC-prohibited payment has been made, the OFAC Advisory does include a clear message that OFAC will consider as "significant" mitigating factors a company's "self-initiated, timely, and complete report of a ransomware attack to law enforcement" as well as the company's "full and timely cooperation with law enforcement."

Key Takeaways from FinCEN Advisory and OFAC Advisory

- Both FinCEN and OFAC continue to reinforce the need to have risk-based compliance programs that incorporate the new and challenging risks posed by ransomware and other types of cyber-attacks.
- Financial intermediaries and those with Bank Secrecy Act ("BSA") obligations must include specific indicators of ransomware attacks in their SARs filings.
- Compliance obligations are not erased by duress of a ransomware attack. Evaluate sanctions risk when making a quick decision to pay a ransomware demand and weigh the risk that the payment may lead to OFAC penalties. Timely and fully report such attacks to law enforcement (and OFAC if its sanctions are implicated).
- If your company has already made a payment, determine whether you have incurred potential OFAC exposure and, if so, consider voluntary disclosure to OFAC.

CONTACTS

David DiBari
Managing Partner
T +1 202 912 5098
E david.dibari
@cliffordchance.com

Megan Gordon
Partner
T +1 202 912 5021
E megan.gordon
@cliffordchance.com

George Kleinfeld
Partner
T +1 202 912 5126
E george.kleinfeld
@cliffordchance.com

Celeste Koeleveld
Partner
T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Daniel Silver
Partner
T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Michelle Williams
Partner
T +1 202 912 5011
E michelle.williams
@cliffordchance.com

Jacqueline Landells
Counsel
T +1 202 912 5061
E jacqueline.landells
@cliffordchance.com

Carol Lee
Associate
T +1 202 912 5194
E carol.p.lee
@cliffordchance.com

Laurence Hull
Associate
T +1 202 912 5560
E laurence.hull
@cliffordchance.com

John-Patrick Powers
Associate
T +1 202 912 5048
E john-patrick.powers
@cliffordchance.com

Holly Bauer
Associate
T +1 202 912 5132
E holly.bauer
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA