Commentary on Ransomware Payments (October 2024)

In the United States, no federal laws have been enacted specifically to limit the payment of cyber ransoms. However, the U.S. Treasury's Office of Foreign Assets Control (OFAC) has explained that such payments may subject ransomware victims to liability under the Trading With The Enemy Act (TWEA) and/or the International Emergency Economic Powers Act (IEEPA). Generally, those laws prohibit U.S. persons from transacting or attempting to transact with an enemy of the U.S., certain related parties, and specified parties subject to U.S. sanctions or embargoes.

OFAC has published two advisories in recent years on the subject of ransomware payments, both of which suggest that U.S. persons may be held strictly liable under TWEA and IEEPA when they make a ransomware payment to a sanctioned person or engage with an embargoed country or region. Strict liability in this context means that any U.S. person may face a civil enforcement action by OFAC for transacting or attempting to transact with an enemy of the U.S. even if the person did not know or have reason to know that a ransomware payment was being made to a sanctioned person or embargoed country or region. Contrary to OFAC's advisories, TWEA and IEEPA and their regulations do not impose a strict-liability standard in all cases where a victim makes a ransomware payment to a threat actor on the Specially Designated Nationals and Blocked Persons list. However, OFAC's interpretation of these statutes and regulations as imposing a strict-liability regime creates substantial uncertainty and unnecessary chilling effects when victims are forced to make ransomware payments. When factors weigh in favor of making the ransomware payment, imposing strict liability is both bad policy and bad law for a ransomware victim, who has no reason to know (and importantly, no time to determine) that the recipient is a sanctioned person or in an embargoed country or region.

This *Commentary* reviews these issues in three parts:

Part 1

An analysis of TWEA and IEEPA; OFAC's recent guidance; and the purported strict-liability standard;

Part 2

A Framework for assisting organizations in identifying the source of an attack and likely recipient of a ransom and evaluating organizations' level of risk from OFAC if the organizations elect to pay; and

Part 3

Suggestions for a more reasoned basis for determining circumstances under which a ransomware payment might be made without the threat of OFAC sanctions.

The full text of *Commentary on U.S. Sanctions-Related Risks for Ransomware Payments*, is available free for individual download from The Sedona Conference website at

https://thesedonaconference.org/publication/Commentary_on_US_Sanctions-Related_Risks_for_Ransomware_Payments