New OFAC Guidance - Ransomware

Client Advisories

10.07.2020

On October 1, 2020, the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") issued a new advisory directed towards financial institutions, cyber insurance companies and companies working in the digital forensic and incident response space about the potential sanctions risks for helping victims make ransomware payments.
OFAC describes "ransomware" as a "form of malicious software designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data." OFAC's advisory indicated that any company or individual who "facilitates" ransomware payments to sanctioned persons, organizations or countries may face civil penalties and/or criminal prosecution. OFAC explained that the demand for ransomware payments has increased multifold during the COVID-19 pandemic as cyber actors target online systems that U.S. persons have relied upon to conduct business remotely.

Generally, OFAC prohibits U.S. persons (both individuals and companies) from engaging in direct and indirect transactions with individuals or entities that OFAC has blocked, and also those transactions covered by OFAC's "comprehensive country or region embargoes." Examples of countries covered by this embargo include, but are not limited to, Venezuela, North Korea, Iran and Cuba.

Notably, OFAC's advisory indicated civil penalties for sanctions violations are established on *strict liability grounds*. Accordingly, "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." Consequently, victims of ransomware attacks should contact OFAC immediately if the attack involves any "sanctions nexus," the guidance said. Victims should also consider informing the Financial Crimes Enforcement Network ("FinCEN"), the Federal Bureau of Investigation ("FBI"), the U.S. Secret Service Cyber Fraud Task Force, the Cybersecurity and Infrastructure Security Agency, and the Homeland Security Investigations Field Office.

Importantly, OFAC indicated it may consider "the existence, nature, and adequacy" of sanctions compliance programs when making an enforcement decision.

Archer attorneys have extensive experience implementing OFAC compliance programs, as well as working alongside of FinCEN, the FBI and Secret Service on behalf of our clients. If you feel OFAC's new ransomware guidance applies to you, and/or your company, and would like more information on the implications of the program, please contact Jeff Kolansky at 215-279-9693 or jkolansky@archerlaw.com.

DISCLAIMER: This client advisory is for general information purposes only. It does not constitute legal or tax advice, and may not be used and relied upon as a substitute for legal or tax advice regarding a specific issue or problem. Advice should be obtained from a qualified attorney or tax practitioner licensed to practice in the jurisdiction where that advice is sought.

Related People

Jeffrey M. Kolansky

Of Counsel

jkolansky@archerlaw.com

215.279.9693

Related Services

- Business Litigation
- Corporate Compliance, Investigations & White Collar Defense
- Data Privacy & Cybersecurity

© 2025 Archer & Greiner, P.C. All rights reserved.