AN A.S. PRATT PUBLICATION
APRIL 2021
VOL. 7 • NO. 3

# PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

# Pratt's Privacy & Cybersecurity Law Report

**VOLUME 7** **NUMBER 3** **April 2021**



LexisNexis®

**QUESTIONS ABOUT THIS PUBLICATION?**

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [69] (LexisNexis A.S. Pratt)



*An A.S. Pratt Publication*
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2021–Pub. 4939)

# *Editor-in-Chief, Editor & Board of Editors*

*Pratt's Privacy & Cybersecurity Law Report* is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices.  For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

# The Treasury Department's Office of Foreign Assets Control Issues Advisory Warning to Victims of Ransomware Attacks

***By David J. Oberly, Jed M. Silversmith, and Matthew J. Thomas****

*The authors of this article discuss a U.S. Department of the Treasury's Office of Foreign Assets Control advisory pertaining to the financial implications of succumbing to ransomware demands and paying money to foreign actors who are subject to U.S. sanctions.*

Ransomware demands have surged during the pandemic. The U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") has issued an advisory pertaining to the financial implications of succumbing to ransomware demands and paying money to foreign actors who are subject to U.S. sanctions. This OFAC guidance underscores the need for a disaster preparedness plan, as well as the need for victims of ransomware attacks to immediately engage counsel to ensure compliance with the law when responding to an attack of this nature.

## OVERVIEW OF RANSOMWARE ATTACKS

Ransomware is a form of malicious software ("malware") designed to block access to a computer system or data, often by encrypting data or programs on information technology ("IT") systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. In some cases, in addition to the attack, the perpetrators will also threaten to publish sensitive files belonging to the victims or their customers. The consequences of a ransomware attack can be severe and far-reaching, with the potential to cause significant losses of sensitive, proprietary, and critical information and/or loss of business functionality.

* David J. Oberly is an associate at Blank Rome LLP, focusing his practice on a broad range of biometric privacy, data privacy, and data security/cybersecurity compliance, risk management, and class action litigation matters. Jed M. Silversmith is of counsel at the firm concentrating his practice in white collar litigation, with a particular focus on civil and criminal tax controversy matters. Matthew J. Thomas is a partner at the firm with more than 25 years of experience in international trade, transport and maritime regulation, and government affairs. The authors may be reached at doberly@blankrome.com, jsilversmith@blankrome.com, and mthomas@blankrome.com, respectively.

Ransomware attacks can impact any business. Given the ongoing pandemic, businesses are relying on IT systems to maintain their daily operations now more than ever. The need for disaster preparedness plans is essential. Any disaster preparedness plan should include responding to a full-blown cyberattack like a ransomware demand, which oftentimes shuts down all of the business' IT infrastructure with no notice.

The Federal Bureau of Investigation ("FBI") has reported a 37 percent annual increase in disclosed ransomware cases between 2018 and 2019, and a 147 percent annual increase in associated losses over the same time period. Although the FBI has not released statistics for 2020, it is widely believed that these figures have increased by even larger margins over the course of the last year. Being ready to respond to a ransomware attack is critical.

## OFAC ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS

OFAC also issued an advisory that addresses some of the compliance issues that arise with ransomware. OFAC's guidance warns companies of the potential risk of violating U.S. sanction laws for making ransomware payments to individuals who are subject to U.S. sanctions.

The OFAC alert[1] reminds companies that the ransom payments, even if made under duress, are still covered by its sanctions regulations, which restrict dealings with certain targeted countries, regions, entities, and persons on grounds such as foreign policy, national security, and combatting weapons proliferation, transnational crime, narcotrafficking, and human rights abuses.

OFAC's sanctions regime prohibits payments to or transactions with specific persons or entities on OFAC's Specially Designated Nationals and Blocked Persons List ("SDN List"), and to certain embargoed countries and regions (e.g., Cuba, Crimea, Iran, North Korea, and Syria) without securing a license. The alert identifies foreign actors in North Korea and Russia who have been recently added to the SDN List because of their involvement with ransomware and other types of malware attacks.

Importantly, the advisory further states that OFAC may impose sanctions "even if [the victim] did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanction laws and regulations administered by OFAC." While most OFAC trade sanctions restrictions apply on a strict liability basis, the alert stresses the importance of disclosure and cooperation with authorities as a key factor in mitigating any potential penalty exposure.

[1] https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001.

Many companies with an international footprint already have an OFAC compliance program. However, many domestic companies that do not regularly conduct business overseas lack a robust compliance program. OFAC's sanctions regime also applies to foreign businesses that utilize U.S. commerce to transact business. All domestic businesses need to be mindful of these obligations. Likewise, foreign businesses, which are just as susceptible to ransomware attacks, need to be aware of their obligations to comply with U.S. sanction laws.

Any business, foreign or domestic, that wishes to send money to someone on the SDN List must obtain a license from OFAC if it involves U.S. commerce. The advisory reiterates the broad reach of U.S. sanction laws:

> Additionally, any transaction that causes a violation . . . , including transactions by a non-U.S. person which causes a U.S. person to violate any . . . sanctions, is also prohibited. U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons, which could not be directly performed by U.S. persons due to U.S. sanctions regulations.

By way of example, V, a foreign company, decides to pay a ransomware payment to company in Iran. That company does not seek a license from OFAC, and instead wires U.S. dollar-denominated funds from its foreign bank account to purchase cryptocurrency to pay the ransom demand. That payment (like most U.S. dollar transactions) clears through a U.S. correspondent bank. As a result, that transaction would violate the OFAC sanction regime and could subject V to a burdensome investigation and potential penalties under U.S. sanctions laws. Worse, if such a transaction was undertaken knowingly or with an intent to evade the sanctions, V also could run afoul of U.S. money laundering, bank, and wire fraud statutes.

## CONCLUSION

Paying a ransomware demand is generally discouraged. However, in some instances companies may make the business decision to meet the financial demands of cyber criminals in order to maintain continuity of operations or protect confidential information from being widely disseminated. OFAC's advisory creates an added layer of complexity and underscores the vital need to prepare for a ransomware attack. The sensitive compliance issues set out in the advisory highlight the benefits of working with experienced counsel, who can guide victims of ransomware in navigating the crisis while ensuring that any actions taken in response do not violate federal law.