# Federal Authorities Warn Employers Against Ransomware Payouts and Offer New Guidance on Preventing and Responding to Cyberattacks

Insights
10.28.21

Federal officials have recently warned employers and businesses that they could have insult added to injury if they respond to cyberattacks by making ransomware payments – increasingly requested through cryptocurrency – as such payments could violate federal law. The U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) issued a September 21 Updated Advisory to stress that the U.S. government strongly discourages companies from making ransomware payments, following up on a 2020 advisory on the potential sanctions they face for facilitating such payouts. The guidance also includes some best practices for your organization to consider to proactively prevent an attack from taking place, and recent federal guidance also provides recommended steps to respond to such an attack. What should your organization know about these critical steps?

**How Did We Get Here?**

In June of this year, the operator of the largest fuel pipeline in the U.S. was hacked by a Russian-affiliated cybercrime group known as DarkSide. The group stole nearly 100 gigabytes of data from U.S. Colonial Pipeline and threatened its release if its ransom was not paid in cryptocurrency (as most cybercriminals currently demand). After reviewing its networks to determine the breadth of the breach, the company shut down the entirety of its gasoline pipeline for the first time in its 57-year history and subsequently paid the requested ransom in the amount of $4.4 million in Bitcoin.

Although the U. S. Department of Justice was able to recover 63.7 of the Bitcoins – worth $2.3 million at the time – the damage was done, and the brazen nature of the attack and its success no doubt will lead other groups to continue their digital assaults on American businesses. The ransomware attack suffered by Colonial Pipeline is not an outlier – and will not remain an aberration – as cyber-attackers are stepping up their work and increasingly demanding payment in cryptocurrency in exchange for the release of a company's systems and data.

Earlier this month, in fact, the Director of the National Security Agency predicted that the U.S. would face a ransomware attack "every single day" within five years. Other cybersecurity experts may be more optimistic about the future outlook, but still recognize that the proliferation of ransomware attacks is a major cause for concern in the business community. This is especially true as the

pandemic's shift leading to a marked increase in employer reliance on technology and remote work has led ransomware attackers to seize the opportunity.

**What Does the Updated Advisory Say?**

Disrupting the financial ecosystem that helps fuel these attacks is a primary area of focus for the Biden administration. It is in furtherance of these efforts that the OFAC released its latest Updated Advisory. Announcing the new guidance, Treasury Secretary Janet Yellen emphasized that "ransomware and cyberattacks are victimizing businesses large and small across America and are a direct threat to our economy" and that "as cybercriminals use increasingly sophisticated methods and technology, we are committed to using the full range of measures, to include sanctions and regulatory tools, to disrupt, deter, and prevent ransomware attacks."

This new advisory provides background on ransomware, gives examples of designated "malicious cyber-actors," and explains how making or facilitating ransomware payments with individuals or entities on the Specially Designated Nationals and Blocked Persons List (SDN List) could violate the OFAC's regulations and result in sanctions.

***Mitigating Factors Considered Before Imposing Sanctions***

The Updated Advisory adds to the first advisory by delineating two mitigating factors the OFAC will consider before imposing sanctions on an employer for facilitating ransomware payments to sanctioned persons or jurisdictions.

- The first is the extent of an **employer's compliance program and defensive measures**. The guidance states that compliance program should take into account that a ransomware payment may involve an entity on the SDN List or a comprehensively embargoed jurisdiction. Given that the OFAC may impose civil penalties based on strict liability, the extent to which the business knew that the entity fell into one of those categories is of little consequence when determining whether to impose sanctions. However, if the business has taken meaningful steps to reduce the risk of exposure to a ransomware attack by adopting good "cyber-hygiene," those steps will be a significant mitigating factor in an OFAC enforcement response.
- The second mitigating factor is the employer's cooperation with the OFAC and law enforcement officials after an attack takes place. Reporting a ransomware payment to the appropriate U.S. government agency and cooperating with the OFAC (as well as law enforcement officials) may help stave off significant enforcement action. The faster an employer self-reports and the greater the extent of their cooperation, the more likely the OFAC will resolve the investigation with what they call a "non-public response," which would not include civil penalties.

***Cryptocurrency Exchange Added to Bad Actors List***

The Updated Advisory also adds SUEX OTC, S.R.O., a cryptocurrency exchange, to the SDN List for its [illegible]

its part in facilitating financial transactions with known ransomware actors. An analysis of Suex's transaction history showed that 40% of its known transactions were associated with illicit actors.

**What Should Employers Do to Prevent Cyberattacks?**

In order to take advantage of the OFAC mitigating factors laid out in the Updated Advisory, your organization should proactively plan ahead and take steps to minimize the chances of a cyberattack. Again, having a **comprehensive compliance program and defensive measures in** place will not only reduce the chances of becoming a cyberattack victim, but will put you in the best position possible under the latest OFAC advisory.

- Provide robust cybersecurity training to employees on an annual basis.
- Require two-factor authorization to access your internal company network.
- Require employees to set up passwords with multiple characters (including numbers, letters, and symbols) and require that the passwords be routinely changed.
- Maintain offline, encrypted backups of your data.
- Regularly test your backups.
- Create, maintain, and exercise a basic cyber-incident response plan, resiliency plan, and associated communications plan. The cyber-incident response plan should include response and notification procedures for ransomware incidents.
- Mitigate internet-facing vulnerabilities and misconfigurations:
    - Employ best practices for use of Remote Desktop Protocol (RDP) and other remote desktop services;
    - Conduct regular vulnerability scanning;
    - Regularly update all operating systems and software, specifically antivirus anti-malware software; and
    - Ensure that devices are properly configured and security features are enabled.

**What Should We Do if Our Company is the Victim of a Ransomware Attack?**

Cyber criminals are increasingly demanding cryptocurrency as payment in ransomware attacks. When considering how quickly data can be digitally shared, being able to decisively respond to an attack can be critical to minimizing damage. As a result, you need to have a plan in place to deal with a potential ransomware attack and know how you will respond should the worst-case scenario occur. If your company becomes the victim of a ransomware attack, the Cybersecurity and Infrastructure Security Agency (CISA) recommends taking the following steps:

- Determine which systems were impacted and immediately isolate them.
- If affected devices cannot be removed from the network (or if the network cannot be temporarily shut down), power infected devices down to avoid further spread of the ransomware infection

shut down), power-infected devices down to avoid further spread of the ransomware infection.

- Triage impacted systems for restoration and recovery.
- Engage your internal and external stakeholders.
- Consider retaining a third-party incident response provider with experience in data breaches.
- Notify affected individuals.
- Report the incident to CISA, your local FBI field office, the FBI Internet Crime Complaint Center, or your local U.S. Secret Service office as soon as possible.
- You should also engage knowledgeable counsel early on to provide guidance during the initial investigation following a ransomware attack and advise on whether the ransomware attack has triggered any data breach notification obligations.

**What Else is the Federal Government Doing to Combat this Rising Threat?**

The White House's use of OFAC sanctions is not the only measure being taken by the Biden administration to crack down on cyberattacks and ransomware crypto payments. In addition, it announced the creation of a ransomware task force in July that will coordinate offensive and defensive resistance measures against ransomware attacks. This effort will include evaluating how to stop payments from being made in cryptocurrencies and how tracing cryptocurrency payments can increase efforts to track attackers, offering rewards in the realm of $10 million to help identify ransomware attackers, launching cyberattacks on hacker gangs, partnering with businesses to better share information about attacks, and coordinating efforts with U.S. allies.

To that end, the White House just hosted over 30 countries for a virtual conference on October 13 focused on combating ransomware attacks. The country delegates in attendance agreed that ransomware attacks are more than a criminal act: they are a transnational security threat. The delegates discussed how they could fight back against cyber criminals and put pressure on the countries that harbor them. These efforts, in tandem with the OFAC's sanctions program, are designed to stem the tide of ransomware attacks.

**Conclusion**

The likelihood that any given employer faces a ransomware attack grows by the day. In addition, the recent rise in many cryptocurrencies to all-time highs only increases the chances of cyber attackers targeting unprepared businesses in the hopes of making an easy score. It is imperative that you are prepared.

Employers must have a sufficient compliance program and robust defensive measures in place, as well as a plan for what to do if your company's data is ever breached. This plan should include access to resources that can manage the cryptocurrency aspects of an attack, if any, steps to curb the attack, determine what data has been accessed, and the process for reporting the attack. Most importantly, employers should exercise caution before engaging with cybercriminals and facilitating ransomware payments. While it may be tempting to pay a ransom to quickly regain access to your

company's data (especially if it's a relatively nominal amount), the end result could be far more costly if you become the subject of an OFAC enforcement action.

Fisher Phillips will continue to monitor further developments in this area, so be sure to subscribe to Fisher Phillips' Insight system to stay up-to-date. If you have any questions regarding how cybersecurity threats could impact your organization, or best practices for addressing those threats, please consult your Fisher Phillips attorney, the authors of this Insight, or a member of Fisher Phillips' Privacy and Cyber Practice Group or our Cryptocurrency and Blockchain Taskforce.

## *Related People*

**Risa B. Boerner, CIPP/US, CIPM**
Partner
610.230.2132
Email

**Phillip C. Bauknight**
Partner
908.516.1059
Email

## *Service Focus*

Privacy and Cyber