CONNECTICUT
EMPLOYMENT LAW LETTER
Part of your Connecticut Employment Law Service

December 2021

# DOJ's new enforcement team may intensify push to recover cyberattack payments

**by Michael L. Yaeger, Joseph W. Swanson, and Erin J. Hoyle, Carlton Fields**

*The U.S. Department of Justice (DOJ) recently announced the launch of a National Cryptocurrency Enforcement Team (NCET) to (1) add structure to and coordinate the agency's investigative capabilities concerning unlawful uses of cryptocurrency, (2) increase prosecutions, and (3) recover illicit proceeds. The last piece is especially striking because it may provide a positive incentive for employers and other cyberattack victims to contact law enforcement and do so quickly. The DOJ stated one NCET focus will be to "assist in tracing and recovery of assets lost to fraud and extortion, including cryptocurrency payments to ransomware groups."*

***Enormous costs***

Cyberattacks using ransomware have caused serious and increasing problems in recent years. The victims have included educational institutions, utilities, hospitals, and other critical infrastructure providers:

- In February 2021, hackers accessed a water treatment plant in Oldsmar, Florida, briefly raising the lye in drinking water to dangerous levels.
- In May, a cyberattack forced Colonial Pipeline Co. to shut down the gasoline supply to much of the Eastern Seaboard, resulting in shortages throughout the South.
- Also in May, an attack shut down a San Diego hospital system's databases for two weeks, significantly disrupting patient care and forcing medical personnel to use paper records.
- In June, an attack on the multinational meat manufacturer JBS S.A. closed a quarter of American beef operations for two days, as the company shut down its computer systems to limit the breach.
- In September, it took Howard University almost three weeks to recover from a ransomware incident that led to several days of canceled classes.

Some commenters estimate more than 65,000 successful ransomware attacks happened in 2020. Around the time of the Colonial Pipeline attack, Homeland Security Secretary Alejandro Mayorkas estimated ransomware groups received $350 million in ransom payments last year.

***Cryptocurrency's key role***

Cryptocurrency plays a significant role in ransomware schemes because attackers prefer it as the method of payment. It allows for the quick transfer of funds internationally and outside of traditional banking systems. Digital asset exchanges are therefore an unsurprising area of scrutiny for regulators and prosecutors. For example, in September, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Suex OTC, S.R.O., a Russian virtual currency exchange, for its alleged role in facilitating and laundering financial transactions for ransomware groups.

Remarkably, on June 7, the DOJ seized 63.7 bitcoins (valued at about $2.3 million) in cryptocurrency ransom paid by Colonial Pipeline. Although such seizures are rare, authorities have gained some experience in tracking the flow of digital money:

- In August 2020, the DOJ announced the seizure of more than 300 cryptocurrency accounts tied to al-Qaida and the Izz ad-Din al-Qassam Brigades, the armed wing of Palestinian militant group Hamas.
- In November 2020, the department revealed the seizure of roughly $1 billion in cryptocurrency associated with the online black market Silk Road.

- In January, the department disclosed the recovery of more than $454,000 in cryptocurrency from the ransomware group NetWalker.

***How ransom money can be tracked***

Although the FBI shared scant details about how it seized a portion of Colonial Pipeline's ransom payment, the broad method by which investigators can at least trace cryptocurrency loot is relatively straightforward:

- Cryptocurrencies are held in digital accounts called wallets, which store addresses for the virtual locations of crypto funds and the private keys, or passwords, to access them.
- The movement of funds between the addresses is recorded in a public ledger called a blockchain.

Crypto wallets provide owners with a measure of personal privacy, but blockchains are visible to the public, enabling investigators to observe the movement of funds between addresses and through exchanges. Should law enforcement gain access to the private key for an address containing a ransom payment, it can obtain a properly issued warrant and seize the portion of the funds making up the stolen amount.

In essence, law enforcement can make a prejudgment seizure, a legal power that private parties generally lack (with a very limited set of exceptions). After seizing the funds, the DOJ can initiate a forfeiture action. The action removes ownership of the funds from the bad actor and, if the government elects to pursue a process called "restoration," returns property obtained under fraudulent pretenses to the victim.

***New enforcement team's goals***

The DOJ intends to have the NCET involved in cryptocurrency and blockchain technologies across all aspects of the department's work. The initiative seeks to employ and build on the work of the agency's Money Laundering and Asset Recovery Section (MLARS) and Computer Crime and Intellectual Property Section (CCIPS) as well as assistant U.S. attorneys detailed from their offices across the country.

If the NCET commits to recovering cyberattack ransom payments, it could create a positive incentive for employers and other victims to contact law enforcement with alacrity. And if the team has any degree of success in its recovery efforts, it could have a big impact on a significant national problem.

*Michael L. Yaeger, Joseph W. Swanson, and Erin J. Hoyle are attorneys with Carlton Fields. You can reach them at myaeger@carltonfields.com, jswanson@carltonfields.com, or ehoyle@carltonfields.com.*