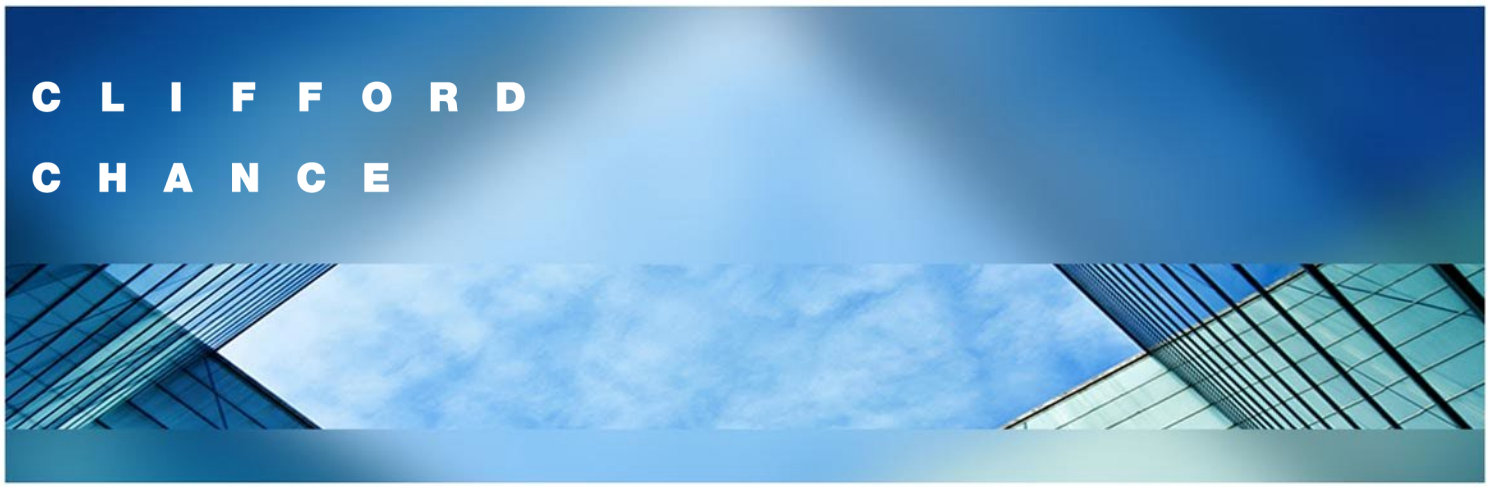

FINCEN FLEXES NEW EXPERTISE IN CLEAR WARNING TO COMPANIES BROADLY INVOLVED IN PROCESSING RANSOMWARE PAYMENTS

The latest study on ransomware from the US Treasury's Financial Crimes Enforcement Network ("**FinCEN**") reflects the US Government's continuing coordinated focus on cybercrime, and ransomware in particular. The study shows increasing ability by FinCEN, and potentially other parts of government, to chart the flow of ransomware payments, particularly in bitcoin, in traditional "follow the money" style, and to identify the most frequently used exchanges and services ransomware actors use to launder their proceeds. According to the study, victims predominantly sourced payment funds from U.S.-registered exchanges and extortionists use foreign centralized convertible virtual currency ("**CVC**") exchanges as their "preferred cash-out points."

On October 15, 2021, FinCEN issued a Report on Ransomware Trends in Bank Secrecy Act Data (the "Ransomware Report"). The study comes out following a wave of governmental action on ransomware, including OFAC's new Sanctions Compliance Guidance for the Virtual Currency Industry[1] as well as its Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments; the White House's release of a multi-government Joint Statement following a summit on ransomware as an escalating global security threat; and the announcement of the Department of Justice's National Cryptocurrency Enforcement Team. All of these actions highlight the importance of ensuring that companies that facilitate cryptocurrency transactions have strong anti-money laundering ("**AML**") compliance programs. The FinCEN report clearly demonstrates the agency is becoming increasingly sophisticated in its ability to identify and track unlawful activity related to cryptocurrency. Companies that facilitate cryptocurrency transactions must strengthen their own detection and monitoring systems to make sure they can identify and prevent suspicious and unlawful transactions or face

Key Takeaways

- FinCEN is becoming increasingly sophisticated in its ability to identify and track unlawful activity related to cryptocurrency.
- FinCEN's Ransomware Study identifies a number of "money laundering typologies" that FinCEN says signal that a transaction may involve ransomware payments.
- Companies that facilitate cryptocurrency transactions—especially those whose transactions relate to the "money laundering typologies" that FinCEN identifies in the report—must strengthen their detection and monitoring systems to make sure they can identify and prevent suspicious and unlawful transactions.
- Ransomware targets that work with digital forensic incident response firms should be aware that those firms will likely need to file a suspicious activity report for any transaction relating to ransomware at or above $2,000.

[1] For more on this publication, see our briefing here.

possible enforcement action. In particular, companies in the ambit of the "ransomware-related money laundering typologies" identified in the FinCEN report—such as foreign centralized exchanges and exchanges that deal with anonymity-enhancing cryptocurrencies or offer services like mixing and decentralized finance ("**DeFi**") applications—should be especially vigilant, both to ensure that they do not facilitate ransomware activity as well as to avoid facing a sanctions enforcement action. Companies that facilitate cryptocurrency transactions should take this opportunity to review their AML compliance programs and make sure they are also in line with OFAC guidance and incorporate best practices for defense, detection and mitigation identified by Treasury.

WHAT THE REPORT INCLUDES

FinCEN's study references and follows upon FinCEN's October 2020 advisory on ransomware. In particular, the new study reflects some of the methodologies FinCEN is using to track ransomware transactions through analysis of suspicious activity reports ("**SAR**") filings and blockchain analysis.

Overall Trends and Findings

FinCEN continues to see various types and sizes of business in several sectors of the economy as reported victims of ransomware. SAR reporting is up 30 percent when comparing the first six months of 2021 with the same period last year. These reports totalled $590 million in suspicious payments, far exceeding the $416 million reported for all of 2020. FinCEN acknowledged that the report consists only of SAR reported information, which it believes does not provide a comprehensive review of all ransomware.[2] Nevertheless, the dramatic increase supports the general consensus among experts that ransomware attacks are occurring with increasing frequency. Interestingly, however, the median amount reported per identified ransomware payment increased by only 2 percent when comparing the two periods—from roughly $100,000 to $102,000. FinCEN reported that most reported payments were for less than $250,000. To the extent that FinCEN is correct in its observation that ransomware actors have shifted to more selective methodologies to target larger enterprises and demand higher payouts, these figures indicate prices victims are currently willing to pay to either unlock their systems or avoid threats to disclose stolen information (a tactic FinCEN describes as "double extortion").

FinCEN's use of blockchain analytics enabled it to identify the 10 most used of roughly 70 variants of software used in the attacks, and the study provides details comparing the frequency of use and dollar amounts of reported suspicious transactions and median incident value, which may serve as a proxy for the median value of ransomware payments associated with each variant. For these top ten variants, the total median incident value was roughly $148,000. FinCEN also identified a set of unique CVC wallet addresses associated with the top 10

[2] The nature of SAR reporting and the fact that not all affected entities may be required to file SARs means the reporting cannot be used to determine the actual amount of payments associated with ransomware. Use of SAR reporting to identify wallets that can be associated with other wallets where ransomware payments might have been processed enabled FinCEN to state that roughly "$5.2 billion in outgoing BTC transactions [are] potentially tied to ransomware payments"; however, FinCEN is not able to provide any understanding of what percentage of this number is indeed ransomware payments.

variants and used for moving payments. These findings highlight FinCEN's investigative ability to track payments in the cryptocurrency space.

Tactics to Evade Detection

SAR reporting indicates that bitcoin is the dominant cryptocurrency used for payment, although attackers increasingly request payment in anonymity-enhanced cryptocurrencies ("**AECs**").[3] FinCEN specifically noted an increase in requests for payments in the AEC Monero (XMR) and the practice of attackers adding "surcharges" if payments were made in bitcoin rather than an AEC. FinCEN also noted the use of The Onion Router ("**Tor**"),[4] email, and unidentified web portals provided by attackers as communication methods to obscure identities and frustrate law enforcement tracking efforts.

FinCEN also identified a number of tactics that attackers use to cover their tracks. This includes avoiding the re-use of wallets for different attacks and using foreign centralized exchanges in high-risk jurisdictions with low anti-money laundering and terrorism financing compliance standards for cash-outs. Attackers also used a variety of tactics to obscure their transaction trail, including using mixing services to comingle ransom payments with "clean" funds, using decentralized exchanges and other DeFi applications, and using "chain hopping," a layering activity involving the conversion from one CVC another, often adding an AEC, such as Monero, into the transaction chain through various CVC exchanges or services. The converted funds are then "transferred to large CVC services and money services businesses with lax compliance programs."

Primary Source of Reporting

Of particular interest is FinCEN's admitted reliance on SARs filed by what FinCEN referred to in its October advisory as digital forensic incident response ("**DFIR**") firms. FinCEN has said that DFIRs may be classified as money transmitters to the extent that they receive and transmit value as part of their incident response services. As such, they would have AML compliance obligations, including SAR reporting obligations, similar to other money transmitters. FinCEN notes that 63 percent of the ransomware-related SARs filed in the first six months of 2021 were submitted by "a small number of DFIR firms" while acknowledging that it does not have information on the total number of DFIRs in existence. One conclusion to draw from this is that FinCEN's ability to track ransomware-related payments may improve, as more DFIRs and other companies that facilitate cryptocurrency transactions comply with their SAR reporting obligations. Indeed, FinCEN indicates that all financial institutions should be alert with respect to trends in ransomware attacks and payment methods and determine when they need to file SARs.

WHAT THIS MEANS FOR INDUSTRY

- FinCEN's specific reference in the report to "large CVC exchanges and money services businesses with lax compliance programs" should be

[3] AECs are cryptocurrencies that provide privacy features such as the ability to obscure the identity of parties to a transaction and limit the ability for third parties to follow the trail of transactions. This in contrast to non-privacy cryptocurrencies like Bitcoin, which allow anyone to view public addresses and transactions on their blockchain networks.

[4] Tor sends a user's internet traffic through a worldwide system of relays, in effect concealing a user's identity and location and making it more difficult to trace internet activity through tools such as network surveillance.

taken as a warning. FinCEN can differentiate levels of activity among CVC exchanges, domestic and foreign, and can use this ability to identify potential for weaknesses in AML compliance or complicity among those exchanges that are preferred vehicles for the cashing out of ransomware payments in bitcoin. Consequently, CVC exchanges need to use crypto analytics tools, as well as red flags and other information outlined in FinCEN's previous guidance to understand and address weaknesses in their systems.

- FinCEN may do further targeting of AECs and the exchanges that provide services with respect to AECs in an attempt to head off increasing use of less transparent vehicles as preferred methods of receipt for ransomware attackers.
- The US "whole of government" approach as well as its focus on international cooperation among US and foreign regulatory, financial intelligence units, and law enforcement counterparts, indicates the likelihood of increasingly coordinated governmental action against actors in the crypto space that may be willingly complicit or may have inadequate anti-money laundering compliance procedures.
- Those in the industry that work with DFIRs should have an understanding that FinCEN appears to consider those entities directly within the scope of FinCEN's regulations, which include obligations to file SARs. A transaction relating to ransomware at or above the $2,000 SAR threshold applicable to money transmitters must be reported to FinCEN.
- To aid in the fight against ransomware attacks and help in FinCEN's continuing analytic efforts, FinCEN recommends financial institutions incorporate indicators or compromise, "(IOCs"), i.e., observable signatures or other details indicating computer or network intrusion, which are available from threat data sources into intrusion detection systems. FinCEN requests that filers include details in SARs of IOCs, information regarding ransomware variants, and other details listed in the report and FinCEN's earlier guidance. FinCEN also suggests immediate contact with law enforcement regarding ransomware activity, and contact with OFAC when the activity or payment may involve a sanctions target.

Good cyber hygiene and risk management starts long before an incident occurs. Clifford Chance has published a number of reports and briefings to help companies protect themselves from attacks and vulnerabilities. For more information, see our Report on What Cyber Regulators Are Saying Around the World as well as our Ransomware Playbook.

CLIFFORD
CHANCE

CONTACTS

Jamal El-Hindi
Counsel

T +1 202 912 5167
E jamal.elhindi
@cliffordchance.com

David DiBari
Partner

T +1 202 912 5098
E david.dibari
@cliffordchance.com

Steven Gatti
Partner

T +1 202 912 5095
E steven.gatti
@cliffordchance.com

Megan Gordon
Managing Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

George Kleinfeld
Partner

T +1 202 912 5126
E george.kleinfeld
@cliffordchance.com

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Philip Angeloff
Counsel

T +1 202 912 5111
E philip.angeloff
@cliffordchance.com

John-Patrick Powers
Counsel

T +1 202 912 5048
E john-patrick.powers
@cliffordchance.com

Carol Lee
Associate

T +1 202 912 5194
E carol.p.lee
@cliffordchance.com

Alex Sisto
Associate

T +1 212 878 4990
E alex.sisto
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com