Cleary Foreign Investment and International Trade Watch

OFAC Ramps up Targeting of Ransomware-linked Actors and FinCEN Updates Ransomware Advisory

By Chase D. Kaniecki, Samuel H. Chang, Michael G. Sanders & Megan Lindgren on November 19, 2021

On November 8, 2021, the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC) **designated** a virtual currency exchange, Chatex, and its infrastructure support providers on the list of Specially Designated Nationals and Blocked Persons (SDN List) for their role in facilitating financial transactions for ransomware actors.**[i]** The Financial Crimes Enforcement Network (FinCEN) also released an **updated advisory** on ransomware and the use of the financial system to facilitate ransomware payments.**[ii]** These actions were taken in furtherance of a coordinated "whole-of-government" effort to disrupt criminal ransomware actors and the virtual currency exchanges used to launder ransom payments around the world.

Designation of Chatex and Related Entities

OFAC's latest round of sanctions, pursuant to **Executive Order 13694**, follow on the heels of the first-ever sanctions imposed against a virtual currency exchange on September 21, 2021, as discussed in our earlier **blog post**.**[iii]** According to OFAC, over half of Chatex's known transaction history was associated with illicit actors, including transactions using the "nested" virtual currency exchange services of recently sanctioned SUEX, whereby SUEX accepted customers upon referral by intermediaries and provided an interface for customers to trade virtual currencies through larger exchanges.

In addition, OFAC, in coordination with Latvian and Estonian government agencies, designated three companies that provided Chatex's operational infrastructure: IZIBITS OU, Chatextech SIA, and Hightrade Finance Ltd. These new designations reflect a further expansion of OFAC's sanctions

targets from virtual currency exchanges to their infrastructure support providers and emphasize OFAC's interest in combating illicit activity, and ransomware in particular, by identifying the networks of bad actors and service providers that profit from them.

Updated FinCEN Advisory

FinCEN published an **advisory** last year to alert financial institutions to trends, typologies, and potential indicators of ransomware, warning that companies involved in facilitating ransomware payments to ransomware perpetrators (including as part of incident remediation) may be engaged in money transmission and thus required to register as a money services business (MSB) with FinCEN and subject to Bank Secrecy Act (BSA) obligations.**[iv]**

The **updated advisory** provides more detail on how virtual currencies are used to facilitate ransomware, as well as additional guidance for financial institutions, including with respect to reporting requirements.**[v]** It explains that cybercriminals are increasingly using unregistered, decentralized convertible virtual currency (CVC) mixing services and anonymity-enhanced cryptocurrencies (AECs), such as Monero, to pass co-mingled CVCs through intermediary accounts and reduce the transparency of CVC financial flows. They may also convert CVCs to legal tender or fiat currency through foreign CVC exchanges with inadequate compliance or regulatory oversight to re-enter the mainstream financial system.

Accordingly, FinCEN identified two new financial red flag indicators of illicit or suspicious activity related to ransomware involving virtual currencies:

1. A customer initiating a transfer of funds involving a mixing service; and
2. A customer using an encrypted network, such as the onion router, or an unidentified web portal to communicate with the recipient of a CVC transaction.

FinCEN also indicated that suspicious transactions associated with ransomware attacks are "situations involving violations that require immediate attention." **[vi]** When a financial institution is required to file a suspicious activity report (SAR) under the BSA for such activity, **[vii]** it must also immediately notify an appropriate law enforcement agency by phone. FinCEN encourages financial institutions to contact its Financial Institution Hotline to report suspicious transactions.

* * *

OFAC and FinCEN are likely to continue to scrutinize the virtual currency industry for abuses related to ransomware. To help detect, prevent, and report suspicious transactions associated with ransomware attacks, U.S. companies should adopt a risk-based approach to compliance and periodically update their policies and procedures and internal controls to incorporate the latest guidance on virtual currencies from OFAC and FinCEN. In particular, banks and MSBs that serve CVC-related customers or that provide CVC-related services should consider (1) integrating red flag indicators of ransomware-related activity into their suspicious activity monitoring systems and (2) ensuring that their suspicious activity reporting policies and practices involve immediate notification of an appropriate law enforcement agency by phone where activity associated with ransomware attacks is deemed to require a SAR

---

[i] *See* Press Release, U.S. Department of the Treasury, "Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange" (Nov. 8, 2021), **https://home.treasury.gov/news/press-releases/jy0471**.

[ii] *See* FinCEN, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" FIN-2021-A004 (Nov. 8, 2021), **https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf**.

[iii] *See* Press Release, U.S. Department of the Treasury, "Treasury Takes Robust Actions to Counter Ransomware" (Sept. 21, 2021), **https://home.treasury.gov/news/press-releases/jy0364**.

[iv] *See* FinCEN, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" FIN-2020-A006 (Oct. 1, 2020), **https://www.fincen.gov/sites/default/files/advisory/2021-11-08/Advisory%20Ransomware%20FINAL%20508_2020%20rescinded.pdf**.

[v] The updated advisory draws on insights from FinCEN's blockchain analysis and recent **Financial Trend Analysis Report**. *See* FinCEN, "Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021," (Oct. 15, 2021), **https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomeware%20508%20FINAL.pdf**.

[vi] *See* e.g., 31 CFR § 1020.320(b)(3) (Banks) and 31 CFR § 1022.320(b)(3) (Money Services Businesses).

[vii] For CVC exchanges that are considered to be MSBs, filing of SARs are required when a transaction is conducted or attempted by, at, or through a MSB, involves or aggregates funds or other assets of at least $2,000 (except as provided in § 1022.320(a)(3)), and the MSB knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part): (i) involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any Federal law or regulation or avoid related transaction reporting requirements; (ii) is designed whether through structuring or other means, to evade any requirements of Chapter 10 or of any other regulations promulgated under the BSA; (iii) serves no business or apparent lawful purpose, and the reporting money services business knows of no reasonable explanation for the transaction after examining the available facts; or (iv) involves use of the MSB to facilitate criminal activity.

Cleary Foreign Investment and International Trade **Watch**