

Banking and Finance Law Daily Wrap Up, CRIMES AND OFFENSES— FinCEN alerts financial institutions to convertible virtual currency scam involving Twitter, (Jul. 17, 2020)

Banking and Finance Law Daily Wrap Up

[Click to open document in a browser](#)

By [J. Preston Carter, J.D., LL.M.](#)

FinCEN's advisory seeks to assist convertible virtual currency exchanges and other financial institutions to identify and report suspicious transactions associated with this type of activity as quickly as possible.

The Financial Crimes Enforcement Network has released an alert regarding the recent high-profile scam exploiting Twitter accounts to solicit fraudulent payments denominated in convertible virtual currency or CVC ([FIN-2020-Alert001](#)). The alert noted that cyber threat actors compromised the accounts of public figures, organizations, and financial institutions to solicit payments to CVC accounts, claiming that any CVC sent to a wallet address would be doubled and returned to the sender. FinCEN added that it was critical that CVC exchanges and other financial institutions identify and report suspicious transactions associated with this type of activity as quickly as possible.

The alert stated that financial institutions should include any relevant technical cyber indicators related to cyber events and associated transactions within the available structured cyber event indicator fields on the Suspicious Activity Report (SAR) form. Any data or information that helps identify the activity as suspicious can be included as an indicator. Examples include chat logs, suspicious IP addresses, suspicious email addresses, suspicious filenames, malware hashes, CVC addresses, command and control (C2) IP addresses, C2 domains, targeted systems, MAC address or port numbers.

FinCEN noted that it is working closely with law enforcement agencies to identify the source of the scams and to disrupt them. If anyone has immediate information to share with law enforcement, that person should contact the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3): <https://www.ic3.gov/default.aspx>.

Last year, FinCEN issued an advisory seeking to assist financial institutions in identifying and reporting suspicious activity related to the exploitation of CVCs for illicit financing purposes. It also released guidance aiming to answer questions concerning the regulatory treatment of certain businesses dealing in CVCs (see [Banking and Finance Law Daily](#), May 10, 2019).

RegulatoryActivity: BankingOperations BankSecrecyAct Blockchain CrimesOffenses FinTech