FinCEN ADVISORY

FIN-2019-A003

May 9, 2019

Advisory on Illicit Activity Involving Convertible Virtual Currency

Criminals continue to exploit virtual currency to support illegal activity, money laundering, and other behavior endangering U.S. national security, including through entities facilitating its anonymous use.

This Advisory should be shared with:

- *Chief Executive Officers*
- *Chief Operations Officers*
- *Chief Risk Officers*
- *Chief Compliance/BSA Officers*
- *BSA/AML Analysts/ Investigators*
- *Information Technology staff*
- *Cybersecurity Units*
- *Fraud Prevention Units*
- *Legal Departments*

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to assist financial institutions in identifying and reporting suspicious activity concerning how criminals and other bad actors exploit convertible virtual currencies (CVCs) for money laundering, sanctions evasion, and other illicit financing purposes, particularly involving darknet marketplaces, peer-to-peer (P2P) exchangers, foreign-located Money Service Businesses (MSBs), and CVC kiosks. Virtual currencies, particularly CVCs, are increasingly used as alternatives to traditional payment and money transmission systems. As with other payment and money transmission methods, financial institutions should carefully assess and mitigate any potential money laundering, terrorist financing, and other illicit financing risks associated with CVCs. This advisory highlights prominent typologies and red flags associated with such activity and identifies information that would be most valuable to law enforcement, regulators, and other national security agencies in the filing of suspicious activity reports (SARs).[1]

The Risks Posed by Virtual Currencies

CVCs may create illicit finance vulnerabilities due to the global nature, distributed structure, limited transparency, and speed of the most widely utilized virtual currency systems. New types of anonymity-enhanced CVCs have emerged that further reduce the transparency of transactions and identities as well as obscure the source of the CVC through the incorporation of anonymizing

1. Many business models of entities dealing with CVC operate as money transmitters. As money transmitters, persons accepting and transmitting CVC are required, like any money transmitter, to register with FinCEN as MSBs and comply with anti-money laundering/countering the financing of terrorism (AML/CFT) program, recordkeeping, and reporting requirements. These requirements apply equally to domestic and foreign-located CVC money transmitters doing business in whole or substantial part within the United States, even if the foreign-located entity has no physical presence in the United States. For more detail on how FinCEN regulations apply to varying business models involving virtual currency, *see* FinCEN Guidance FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," May 9, 2019 ("2019 CVC Guidance").

features, such as mixing and cryptographic enhancements.[2] Some CVCs appear to be designed with the express purpose of circumventing anti-money laundering/countering the financing of terrorism (AML/CFT) controls. All of these factors increase the difficulty for law enforcement and other national security agencies' efforts to combat money laundering, terrorist financing, and other financial crimes facilitated through CVC.

A financial institution that fails to comply with its AML/CFT program, recordkeeping and reporting obligations, as well as other regulatory obligations, such as those administered by the Office of Foreign Assets Control (OFAC), risks exposing the financial system to greater illicit finance risks. This is particularly true among unregistered MSBs that may be attempting to evade supervision and fail to implement appropriate controls to prevent their services from being leveraged in money laundering, terrorist financing, and other related illicit activities. Without sufficient controls in place, financial institutions cannot reasonably assess and mitigate the potential risks posed by a customer's source of funds or a customer's counterparty, and criminals can exploit the U.S. financial system by engaging in illicit transactions. Individuals engaged in illicit activity will continue to exploit these vulnerabilities as long as the perceived risk of detection is less than that of using traditional financial institutions.

The prevalence of unregistered CVC entities without sufficient AML/CFT controls and the limited transparency of CVC transactions makes CVCs an attractive method of money transmission by those engaged in illicit conduct and other criminal acts that threaten U.S. national security. According to FinCEN's analysis of BSA and other data, illicit actors have used CVCs to facilitate criminal activity such as human trafficking, child exploitation, fraud, extortion, cybercrime, drug trafficking, money laundering, terrorist financing, and to support rogue regimes and facilitate sanctions evasion. Additionally, the increased use of CVC has made legitimate users and financial intermediaries the target of sophisticated cyber intrusions aimed at theft of CVC. Of particular concern is that CVC has come to be one of the principal payment and money transmission methods used in online darknet marketplaces that facilitate the cybercrime economy.[3]

Virtual Currency Abuse Typologies

FinCEN and U.S. law enforcement have observed unregistered entities being exploited or wittingly allowing their platforms to be utilized by criminals in the United States and abroad to further illicit activity, including through darknet marketplaces, P2P exchangers, foreign-located MSBs, and CVC kiosks.[4]

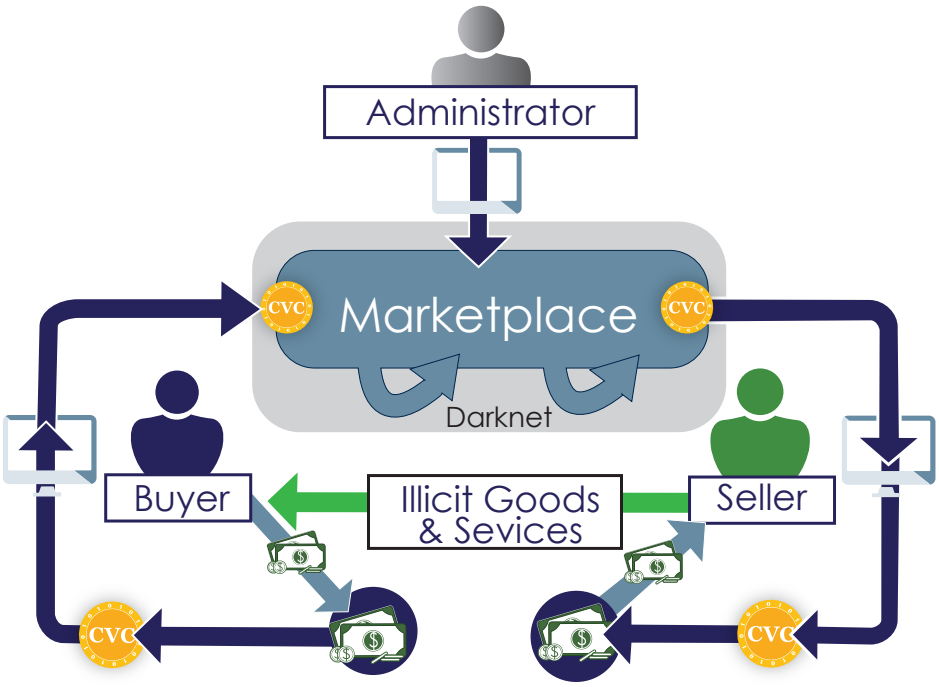
2. Mixing or tumbling involves the use of mechanisms to break the connection between an address sending CVC and the addresses receiving CVC.

3. Darknet marketplace content is not indexed by traditional search engines and requires unique software or authorization to access. *See* Federal Bureau of Investigation, "A Primer on DarkNet Marketplaces: What They Are and What Law Enforcement is Doing to Combat Them," Nov. 1, 2016; *see also* U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, "ICE Investigators Expose Darknet Criminals to the Light," last updated Nov. 2017.

4. The typologies and red flags discussed in this advisory apply to any decentralized ledger-based currency or CVC.

Darknet Marketplaces

Darknet marketplaces are websites that are only available in anonymized overlay networks that require specific software to access.[5] Some require additional vetting or configurations to access. These marketplaces frequently include offers for the sale of illicit goods and services and specify virtual currency as a method – sometimes the sole method – of payment. The use of CVC in conjunction with darknet market activity may indicate drug purchases or sales, child exploitation, cybercrime, or other criminal activity. Accordingly, detectable darknet marketplace linkages, such as through a customer's online behavior, may indicate CVC use in support of illicit activity. Additionally, darknet marketplaces often directly facilitate transactions denominated in CVC to facilitate purchases of goods or services. Entities facilitating the transmission of CVCs are required to register with FinCEN as an MSB. If such an entity has not registered with FinCEN, it may be operating illegally as an unregistered MSB.



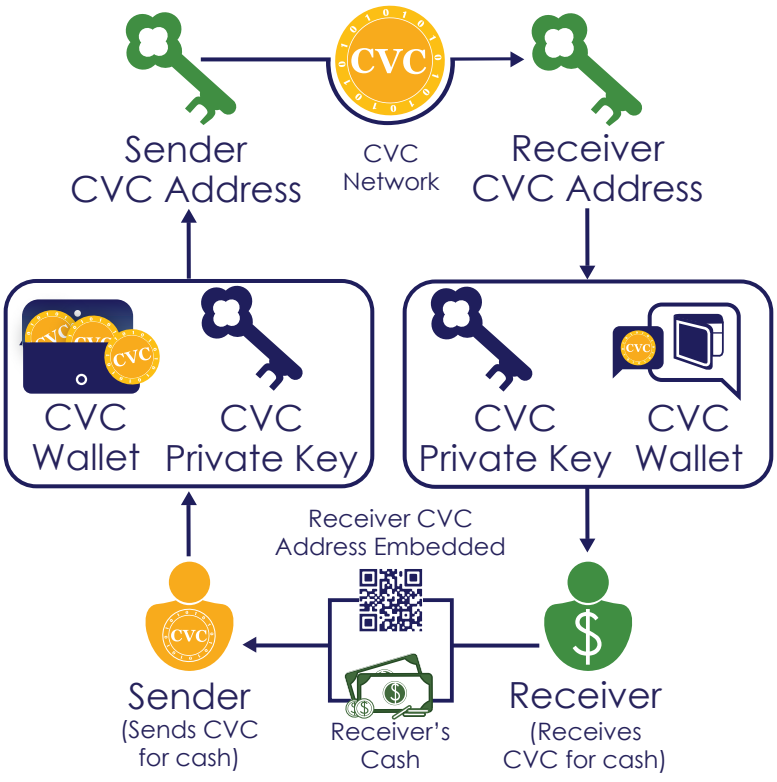
Darknet Marketplace—AlphaBay and Alexandre Cazes (a.k.a. Alpha02, Admin): In July 2017, U.S. law enforcement agencies announced a multi-national effort that dismantled AlphaBay, the largest criminal darknet market in operation at the time. On July 5, 2017, Thai authorities, on behalf of the United States, arrested Alexandre Cazes for his role as the creator and administrator of AlphaBay on charges that included conspiracy to commit identity theft, distribution of narcotics, and money laundering conspiracy. AlphaBay operated as a hidden service on the Tor network to hide the locations of its underlying servers and the identities of its administrators, moderators, and users. In a two-year span, AlphaBay was used by hundreds

5. An overlay network is a telecommunications network that is built on top of another network and is supported by its infrastructure. The Onion Router (Tor) network, accessible through specialized software, is an example of an overlay network.

of thousands of people to buy and sell illegal drugs (e.g., fentanyl and heroin), in addition to other illicit products, often through transactions denominated in CVCs such as bitcoin, monero, and ether.[6] U.S. law enforcement authorities worked with international partners to freeze and preserve millions of dollars' worth of CVC-denominated proceeds of AlphaBay's illegal activities that were subject to forfeiture counts in the indictment.[7]

Unregistered Peer-to-Peer (P2P) Exchangers

P2P exchangers are individuals or entities offering to exchange fiat currencies for virtual currencies or one virtual currency for another virtual currency. P2P exchangers usually operate informally, typically advertising and marketing their services through online classified advertisements, online forums, social media, and through word of mouth. P2P exchangers may provide their services online, or may arrange to meet prospective customers in person to purchase or sell virtual currency.



As explained in FinCEN's recent Guidance issued on May 9, 2019, in undertaking these activities, P2P exchangers function as MSBs and, therefore, must comply with all requirements for MSBs under the Bank Secrecy Act (BSA) and its implementing regulations.[8] FinCEN is aware of cases in which unregistered entities fraudulently represent themselves as individual account holders or misrepresent the nature of their business to conceal their money transmission activity and avoid MSB AML/CFT requirements.

Some P2P exchangers employ techniques, such as mixing or the use of money mules, to further conceal or anonymize transactions. Mixing refers to mechanisms that allow a CVC user to mask their identity through blending the proceeds of their transaction with those of other users. Money mules refer to third parties used to carry out transactions on behalf of another individual.[9]

6. AlphaBay had approximately 200,000 users, 40,000 vendors, 250,000 listings, and facilitated more than $1 billion in CVC transactions between 2015 and 2017. *See* U.S. Department of Justice Press Release, "AlphaBay, the Largest Online 'Dark Market,' Shut Down," July 20, 2017.
7. *See* U.S. Department of Justice Press Release, "AlphaBay, the Largest Online 'Dark Market,' Shut Down," July 20, 2017.
8. *See* 2019 CVC Guidance, at 14-15.
9. *See also supra*, at 2 n.2.

Financial institutions may identify P2P exchangers through perceived funnel account activity, as many of the P2P exchangers' clients deposit funds into the P2P exchanger's account.[10] Financial institutions may be able to distinguish P2P exchangers from traditional funnel account activity by identifying frequent interactions with CVC-focused MSBs.

P2P exchangers are distinct from online P2P trading platforms that match potential virtual currency buyers and sellers with one another in order to facilitate in-person, direct exchanges between individuals. Some buyers and sellers also engage in ongoing, repeated exchange transactions, thereby operating as small-scale unregistered CVC exchangers. Recent cases suggest that CVC buyers and sellers involved in small-volume exchanges are increasingly used for money laundering purposes, possibly without their knowledge, such as to launder proceeds from drug trafficking.[11]

Unregistered P2P Exchanger—Eric Powers: On April 18, 2019, FinCEN assessed a $35,350 civil money penalty against Eric Powers for willfully violating the BSA's registration, program, and reporting requirements during his operations as a P2P exchanger of CVC. The action included an industry bar that prohibits him from providing money transmission services or engaging in any other activity that would make him a "money services business" for purposes of FinCEN regulations. This was FinCEN's first enforcement action against a P2P CVC exchanger. Powers failed to register as an MSB, had no written policies or procedures for ensuring compliance with the BSA, and failed to report suspicious transactions and currency transactions. He advertised his intent to purchase and sell bitcoin on the Internet and completed transactions by either physically delivering or receiving currency in person, sending or receiving currency through the mail, or coordinating transactions by wire through a depository institution. Powers processed numerous suspicious transactions without ever filing a SAR, including doing business related to the illicit darknet marketplace "Silk Road," as well as servicing customers through Tor without taking steps to determine customer identity and whether funds were derived from illegal activity. Powers conducted over 200 transactions involving the physical transfer of more than $10,000 in currency, yet failed to file a single CTR.[12]

P2P Exchangers Facilitating Malicious Cyber Activity—Ali Khorashadizadeh and Mohammad Ghorbaniyan: On November 28, 2018, OFAC took action against two Iranian individuals operating as digital currency[13] P2P exchangers, Ali Khorashadizadeh and

10. For a detailed description of funnel accounts, *see* FinCEN Advisory, FIN-2014-A005, "Update on U.S. Currency Restriction in Mexico: Funnel Accounts and TBML," May 28, 2014.
11. For examples of cases involving P2P trading platforms, *see* U.S. Department of Justice Press Release, U.S. Attorney's Office Western District of New York, "Rochester Man Pleads Guilty in Case Involving Bitcoins, " April 27, 2017; *see also* U.S. Department of Justice Press Release, U.S. Attorney's Office District of Arizona, "Arizona-Based Peer-to-Peer Bitcoin Trader Convicted of Money Laundering, Mar. 29, 2018"
12. *See* FinCEN Press Release, "FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws," April 18, 2019.
13. For the purposes of OFAC sanctions programs, "digital currency" includes sovereign cryptocurrency, virtual currency, and digital representations of fiat currency. *See* U.S. Department of the Treasury Resource Center, "OFAC FAQs: Sanctions Compliance – Questions on Virtual Currency."

Mohammad Ghorbaniyan, helped exchange bitcoin ransom payments into Iranian rial on behalf of malicious Iranian cyber actors involved with the SamSam ransomware scheme that targeted over 200 known victims. As part of these designations, OFAC identified two digital currency addresses associated with these designated Iranian financial facilitators. This marked OFAC's first public attribution of digital currency addresses to designated individuals.[14]

Unregistered Foreign-Located MSBs

Foreign-located MSBs, like P2P exchangers, offer to exchange fiat and CVCs. They may also accept one type of CVC and transmit the same or a different type of CVC to a different person or location. A foreign-located business qualifies as an MSB if it does business as an MSB "wholly or in substantial part within the United States."[15] Foreign-located MSBs seeking to avoid regulatory coverage generally choose to operate in jurisdictions that lack or have limited AML/CFT laws governing the use of CVC. These foreign-located MSBs often do not comply with the AML/CFT regime of the United States, despite doing business wholly or in substantial part within the United States. Foreign-located MSBs that do not adhere to AML/CFT requirements and standards are popular among illicit users of CVC seeking to move funds in and out of the United States and represent a significant money laundering vulnerability. Further, the absence of effective AML/CFT regulatory and supervisory frameworks for CVC activities across jurisdictions can exacerbate illicit financing risks and may create opportunities for legal and regulatory arbitrage.

Unregistered Foreign-Located MSB—BTC-e (a.k.a. Canton Business Corporation) and Alexander Vinnik: In January 2017, BTC-e and its alleged owner and operator, Alexander Vinnik, were indicted in the U.S. District Court for the Northern District of California for operating an unlicensed MSB, conspiracy to commit money laundering, money laundering, and engaging in unlawful monetary transactions. Further, FinCEN simultaneously imposed civil money penalties on BTC-e and Alexander Vinnik of $110,003,314 and $12,000,000 respectively for willful violations of the BSA and its implementing regulations.[16] BTC-e was a foreign-located money transmitter doing business in the United States that exchanged fiat currency as well as CVCs such as bitcoin, litecoin, namecoin, novacoin, peercoin, ether, and dash. It was among the largest virtual currency exchanges by volume in the world. In addition to being an unlicensed MSB, BTC-e and Vinnik failed to comply with their AML program, reporting, and recordkeeping obligations, including the obligation to know your customer (KYC). BTC-e and Vinnik provided users and transactions anonymity by allowing users to access their services

14. *See* Treasury Press Release, "Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses," Nov. 28, 2018.
15. 31 U.S.C. §§ 5312(a)(6), 5312(b), and 5330(d); 31 C.F.R. § 1010.100(ff).
16. *See* FinCEN Assessment of Civil Money Penalty, "Assessment of Civil Money Penalty In the matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik," July 2017.

indirectly through a system of BTC-e shell companies and affiliate entities. The structure of BTC-e and its business dealings made it a leading outlet for money laundering among criminals, including cybercriminals. BTC-e facilitated transactions involving ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking. From 2011 through 2017, BTC-e processed several billion dollars in exchanges.[17]

CVC Kiosks

CVC kiosks (also called bitcoin Automated Teller Machines (ATMs) or crypto ATMs) are ATM-like devices or electronic terminals that allow users to exchange cash and virtual currency. CVC kiosks generally facilitate money transmission between a CVC exchange and a customer's wallet or operate as a CVC exchange themselves. While some kiosk operators have registered and implemented AML/CFT controls, other kiosks have operated in ways that suggest a willful effort to evade BSA requirements. For example, some kiosk operators have assisted in structuring transactions, failed to collect and retain required customer identification information, or falsely represented the nature of their business—for instance by claiming involvement in cash intensive activities—to their CVC exchange and depository institutions.

CVC Kiosks—Khalil Wright: In 2017, the U.S. District Court for the District of Maryland sentenced Khalil Wright to two years' imprisonment for possession with intent to distribute a controlled substance. During the course of the investigation underlying the conviction, law enforcement obtained evidence that Wright purchased at least $112,797 of bitcoin from a bitcoin kiosk in Baltimore, Maryland and sent the bitcoin purchased at the kiosk directly to AlphaBay, a now-defunct darknet marketplace that facilitated drug sales.[18]

Red Flag Indicators of the Abuse of Virtual Currencies

CVC-focused MSBs and other financial institutions can play key roles in identifying unregistered MSB activity and suspicious virtual currency purchases, transfers, and transactions through the application of certain red flags or indicators of illicit conduct. As no single red flag is necessarily indicative of CVC activity linked to illicit conduct, institutions should consider additional contextual information and the surrounding facts and circumstances, such as a customer's historical financial activity and whether the customer exhibits multiple indicators before determining that CVC activity is suspicious. When evaluating potential suspicious activity,

17. *See* U.S. v. BTC-e, A/K/A Canton Business Corporation and Alexander Vinnik (Jan. 2017).

18. *See* United States v. Khalil Wright, No. 1:16-mj-02987 (Nov. 2016).

institutions should be mindful that some red flags might be more readily observable during general transactional screening, while others may be more readily observable during transaction-specific reviews.

Darknet Marketplaces

1. A customer conducts transactions with CVC addresses that have been linked to darknet marketplaces or other illicit activity.
2. A customer's CVC address appears on public forums associated with illegal activity.
3. A customer's transactions are initiated from IP addresses associated with Tor.
4. Blockchain analytics indicate that the wallet transferring CVC to the exchange has a suspicious source or sources of funds, such as a darknet marketplace.
5. A transaction makes use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces.

Unregistered or Illicitly Operating P2P Exchangers

6. A customer receives multiple cash deposits or wires from disparate jurisdictions, branches of a financial institution, or persons and shortly thereafter uses such funds to acquire virtual currency.
7. A customer receives a series of deposits from disparate sources that, in aggregate, amount to nearly identical aggregate funds transfers to a known virtual currency exchange platform within a short period of time.
8. Customer's phone number or email address is connected to a known CVC P2P exchange platform advertising exchange services.

Unregistered Foreign-Located MSBs

9. A customer transfers or receives funds, including through traditional banking systems, to or from an unregistered foreign CVC exchange or other MSB with no relation to where the customer lives or conducts business.
10. A customer utilizes a CVC exchanger or foreign-located MSB in a high-risk jurisdiction lacking, or known to have inadequate AML/CFT regulations for CVC entities, including inadequate KYC or customer due diligence measures.
11. A customer directs large numbers of CVC transactions to CVC entities in jurisdictions with reputations for being tax havens.

12 A customer that has not identified itself to the exchange, or registered with FinCEN, as a money transmitter appears to be using the liquidity provided by the exchange to execute large numbers of offsetting transactions, which may indicate that the customer is acting as an unregistered MSB.

Unregistered or Illicitly Operating CVC Kiosks

13 A customer operates multiple CVC kiosks in locations that have a relatively high incidence of criminal activity.

14 Large numbers of transactions from different customers sent to and from the same CVC wallet address but not operating as a known CVC exchange.

Illicit Activity Leveraging CVC Kiosks

15 Structuring of transactions just beneath the CTR threshold or the CVC kiosk daily limit to the same wallet address either by using multiple machines (i.e., smurfing) or multiple identities tied to the same phone number.

Other Potentially Illicit Activity

16 A customer conducts transactions with CVC addresses that have been linked to extortion, ransomware, sanctioned CVC addresses, or other illicit activity.

17 A customer's transactions are initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious.

18 Use of virtual private network (VPN) services or Tor to access CVC exchange accounts.

19 A customer initiates multiple rapid trades between multiple virtual currencies with no related purpose, which may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction.

20 A customer provides identification or account credentials (e.g., non-standard password, IP address, or flash cookies) shared by another account.

21 A customer conducts transactions or rapidly executes multiple conversions between various types of different CVCs below relevant due diligence, recordkeeping, or reporting thresholds and then transfers the value off of the exchange.

22 Discrepancies arise between IP addresses associated with the customer's profile and the IP addresses from which transactions are being initiated.

23 A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a CVC money mule or a victim of elder financial exploitation.

24 A customer shows limited knowledge of CVC despite engagement in CVC transactions or activity, which may indicate a victim of a scam.

25 A customer declines requests for "know your customer" documents or inquiries regarding sources of funds.

26 A customer purchases large amounts of CVC not substantiated by available wealth or consistent with his or her historical financial profile, which may indicate money laundering, a money mule, or a victim of a scam.

27 A common wallet address is shared between accounts identified as belonging to two different customers.

28 Deposits into an account or CVC address significantly higher than ordinary with an unknown source of funds, followed by conversion to currency of legal tender, which may indicate theft of funds.

29 Multiple changes to email address and other contact information for an account or customer which may indicate an account takeover against a customer.

30 Use of language in CVC message fields indicative of the transactions being conducted in support of illicit activity or in the purchase of illicit goods, such as drugs or stolen credit card information.

Valuable Information in Reporting Suspicious Activity Involving CVC

CVC transactions generate a significant variety of information elements that may be extremely useful to law enforcement and other national security agencies in investigating potential illicit conduct involving CVC transactions. Specifically, the following information is particularly helpful to law enforcement:

- virtual currency wallet addresses
- account information
- transaction details (including virtual currency transaction hash and information on the originator and the recipient)
- relevant transaction history
- available login information (including IP addresses)
- mobile device information (such as device IMEI)
- information obtained from analysis of the customer's public online profile and communications.

When filing a SAR, financial institutions should provide all pertinent available information in the SAR form and narrative.

Reminder of Regulatory Obligations for U.S. Financial Institutions Regarding Suspicious Activity Reporting and Illicit Activity Involving CVC

Suspicious Activity Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.[19] Suspicious activity involving CVC may be observable by financial institutions specializing in commerce related to CVC, financial institutions servicing such businesses, or financial institutions with customers actively involved in the use of CVC.

Because some red flags associated with abuse of CVC may reflect legitimate financial activities, financial institutions should evaluate indicators of potential CVC misuse in combination with other red flags and the expected transaction activity before determining that a particular transaction is suspicious. Due to the technical nature of blockchain analysis and other frameworks of analyzing CVC activity, FinCEN encourages communication within financial institutions among AML, fraud and information technology departments, as appropriate. FinCEN also encourages communication among financial institutions under the auspices of Section 314(b) of the USA PATRIOT Act in determining transactions' potential suspiciousness related to terrorist financing or money laundering activities, and in filing SARs, as appropriate.

SAR Filing Instructions

FinCEN requests that financial institutions reference this advisory by including the key term:

"CVC FIN-2019-A003"

in the SAR narrative to indicate a connection between the suspicious activity being reported and possible illicit activity involving CVC. Using the new, mandatory SAR Form that took effect on January 1, 2019, financial institutions should reference this advisory using the above key term in SAR field 2 ("Filing Institution Note to FinCEN").

19. *See generally* 31 CFR §§ 1010.320, 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.

OFAC Obligations[20]

U.S. individuals and institutions involved in digital currency use or transactions should be aware of their responsibilities for ensuring that they do not engage in unauthorized transactions prohibited by OFAC. OFAC sanctions requirements include not only screening against OFAC's Specially Designated Nationals (SDN) list, but also undertaking appropriate steps to prohibit persons in sanctioned countries and jurisdictions from opening accounts and trading in digital currency. Businesses and entities dealing in digital currency should implement policies and procedures that allow them to: block IP addresses associated with a sanctioned country or region; disable the accounts of all holders identified from a sanctioned country or region; install a dedicated Compliance Officer with authority to ensure compliance with all OFAC-administered sanctions programs; screen all prospective users to ensure they are not from geographic regions subject to U.S. sanctions; and ensure OFAC compliance training for all relevant personnel.

For Further Information

Questions or comments regarding the contents of this advisory should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day). The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

Financial institutions or virtual currency providers having questions concerning OFAC sanctions should either call OFAC's Toll-Free Hotline at 1-800-540-6322 or email OFAC's Feedback Account at OFAC_Feedback@treasury.gov

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

20. U.S. persons, including U.S. financial institutions, have other regulatory obligations as well, including the obligation to comply with U.S. sanctions. The Office of Foreign Assets Control issued guidance specific to digital currency, including CVCs, in March 2018 (*see* Treasury Resource Center, "OFAC FAQs: Sanctions Compliance – Questions on Virtual Currency").