Dechert LLP

ON**POINT** / A legal update from Dechert

MAY 2019

Financial Crimes Enforcement Network, Treasury Department Affirm Regulatory Regime for Convertible Virtual Currencies

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued guidance on May 9, 2019, underscoring the application of the Bank Secrecy Act (BSA) and its implementing regulations relating to money services businesses (MSBs)[1] to certain businesses that transact in convertible virtual currencies (CVCs).[2] On the same day, FinCEN issued an advisory to assist financial institutions in identifying and reporting illicit activity involving CVCs. The advisory highlights certain "red flags" with which financial institutions should become familiar in crafting their anti-money laundering (AML) policies. The guidance consolidates current FinCEN regulations and related administrative rulings and guidance issued since 2011 and then applies these rules and interpretations to common CVC business models. While FinCEN noted the guidance "does not establish any new regulatory expectations or requirements," it was just one of several outreach efforts to the industry since the beginning of May – an indication that the Treasury Department is prioritizing issues involving the potential misuse of CVCs to facilitate money laundering, sanctions evasion and other illicit finance schemes.

FinCEN Guidance

The guidance issued by FinCEN may not have established new regulatory requirements, but – in conjunction with a recent FinCEN enforcement action against an individual operating as peer-to-peer exchanger – it demonstrates the many ways that FinCEN's regulatory regime can extend to the virtual currency industry.

- **Persons or entities engaged in the business of money transmission or the transfer of funds – including CVCs – are MSBs**.[3] FinCEN has long assumed an expansive definition of what constitutes "money transmission services" under the BSA, to encompass the acceptance or transmission of currency, funds, or other value that substitutes for currency. FinCEN's guidance makes clear that its regulations do not limit or qualify the scope of "value that substitutes for currency," and that transactions denominated in CVCs qualify.
- **The label applied to any particular CVC is not dispositive of its regulatory treatment**. FinCEN will not distinguish between "digital currencies," "digital assets," "cryptocurrencies," "cryptoassets" or any other virtual currency instrument. It only matters that the CVC itself has an equivalent value as currency or acts as a substitute for currency in some fashion, and thus is a "value that substitutes for currency."
- **The activities determine MSB status under FinCEN regulations**. As demonstrated by FinCEN's recent enforcement action (cited above), it does not matter whether it is a person or entity engaging in money transmission services, nor does it matter whether a person or entity's activities are licensed as a business. FinCEN will look strictly at whether any person or entity is operating as an MSB.

FinCEN's guidance goes on to discuss how and whether several businesses operating or dealing in CVC – including peer-to-peer (P2P) exchangers, wallet providers, CVC kiosks (commonly referred to as "CVC

automatic teller machines (ATMs)",[4] anonymity-enhanced CVCs, payment processors, and internet casinos – might qualify as MSBs, depending on their specific characteristics. The determination of whether a person is a money transmitter under the BSA regulations is a matter of facts and circumstances. In most cases, the determining factor is whether the business has or assumes custody or control over the CVC at any stage of a transmission for value. Businesses involved in the CVC industry should continue to evaluate their business model and consider whether their activities fall within reach of BSA regulations.

The guidance also lists specific business models involving virtual currencies that may be exempt from the definition of money transmission, including currency trading platforms, decentralized exchanges, initial coin offerings, virtual currency miners conducting transactions with their own currency and transmission by mining pools and cloud miners.

FinCen Advisory

The advisory highlights threats posed by the criminal exploitation of CVCs for money laundering, sanctions evasion or other illicit financing purposes, and provides identification and reporting guidance for financial institutions. Among other things, the advisory describes risks associated with (i) "darknet marketplaces,"[5] (ii) P2P exchanges, (iii) unregistered foreign-located MSBs, and (iv) CVC kiosks. The advisory also sets forth a list of 30 red flags of potential abuses using CVC, including: a customer's receipt of multiple deposits from different sources in a relatively short time, which in total equal the aggregate amount of funds transferred to a known virtual currency exchange; a customer's transactions emanating from a non-trusted IP address; an IP address associated with a sanctioned jurisdiction or an IP address previously identified as suspicious; and a customer using identification or account credentials employed by another account. FinCEN encourages financial institutions to work with their AML, fraud and information technology departments in analyzing CVC activities, due to the complex nature of the underlying technology.

The advisory also provides financial institutions with guidance on suspicious activity reporting relating to CVCs and the types of information that will be required and helpful to law enforcement. For example, wallet addresses, available login information (including IP addresses) and mobile device information (such as device IMEI number) should be included in all suspicious activity reports involving CVC that are filed with FinCEN. The advisory also requests that financial institutions filing suspicious activity reports reference the advisory itself (CVC FIN-2019-A003) on the SAR form if there is a connection between the suspicious activity report and illicit activity involving CVC.

Industry Outreach

Days after FinCEN issued its updated guidance, Sigal Mandelker, the Under Secretary of the Treasury for Terrorism and Financial Intelligence, delivered public comments emphasizing many of the same points. In highlighting the legal and regulatory obligations for CVC businesses operating as MSBs, Under Secretary Mandelker made special note of CVC trading platforms, administrators, CVC kiosks, CVC precious metals dealers and individual peer-to-peer exchangers. The Under Secretary also made a point of focusing on the potential for individual liability for actors who "egregiously flaunt their obligations" – a theme that echoes recent guidance issued by the Office of Foreign Assets Control (OFAC) with regard to potential sanctions violations.

Under Secretary Mandelker's remarks capped a flurry of recent engagement with the CVC industry. In early May, FinCEN hosted an information exchange with the industry and law enforcement to share methodologies used by illicit actors, and the Financial Action Task Force – the international standards setting body for AML and illicit finance issues, currently chaired by the United States – hosted a private sector forum with CVC businesses to discuss compliance. Under Secretary Mandelker herself noted the CVC industry's collaborative role in policing emerging technologies from misuse, citing the fact that CVC exchangers or administrators were responsible for filing "half" of the approximately 47,000 SARs mentioning CVCs since 2013.

Nonetheless, it is clear that FinCEN (and the Treasury Department more broadly) are paying closer attention to issues surrounding CVCs, and emphasizing compliance with existing laws and regulations. While FinCEN has stressed a collaborative approach to the CVC industry, it would be reasonable to expect increased policing in this area, given that Under Secretary Mandelker has also overseen a recent uptick in enforcement actions brought by FinCEN's sister agency, OFAC, for U.S. sanctions violations.

Conclusion

Although the recent releases from FinCEN are not presented as new or groundbreaking, they do clarify significant priorities relating to CVCs. In general, parties in decentralized transactions, whether over

exchanges, P2P or involving anonymized software or virtual currencies, will not be money transmitters required to comply with BSA obligations unless engaged in money transmission. Financial institutions, administrators, exchangers, wallet providers and others should use this opportunity to revisit their own business models, review the applicability of various laws and regulations administered by both FinCEN and OFAC, and update their risk assessments and compliance programs.

Footnotes

1) FinCEN defines "money service business" as "a person, wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part in the United States," who functions as (among other things) a "money transmitter," or a person engaged in "money transmission services". The guidance notes that "money transmission services" include the acceptance of "value that substitutes for currency" from one person and the transmission of "value that substitutes for currency" to another location or person by any means.

2) CVC is a type of "value that substitutes for currency."

3) MSBs must: (1) register with FinCEN; (2) develop, maintain, and implement an "effective" written AML program; (3) detect and adequately report suspicious transactions through the submission of suspicious activity reports (SARs); and (4) file currency transactions reports, where applicable. MSBs must also comply with a host of other AML reporting and record keeping obligations that apply to "financial institutions" under BSA regulations.

4) CVC kiosks are electronic terminals that act as mechanical agencies of the owner-operator to enable the owner-operator to facilitate the exchange of CVC for fiat currency or other CVC.

5) Darknet marketplaces reference anonymized locations on the Internet that are not indexed by traditional search engines, and typically require special software to access.

This update was authored by:

Jeremy B. Zucker
Partner, Washington, D.C.
T: +1 202 261 3322
jeremy.zucker@dechert.com

Sean Kane
Counsel, Washington, D.C.
T: +1 202 261 3407
sean.kane@dechert.com

Robin Nunn
Partner, Washington, D.C.
T: +1 202 261 3401
robin.nunn@dechert.com

Timothy Spangler
Partner, Orange County/Silicon Valley
T: +1 949 442 6044
T: +1 650 813 4803
timothy.spangler@dechert.com

Andrew Schaffer
Associate, New York
T: +1 212 649 8717
andrew.schaffer@dechert.com

Matthew Keehn
Associate, New York
T: +1 202 261 3302
matthew.keehn@dechert.com