POLICY ALERT // MAY 20, 2019

FATF Pushing to Strengthen Regulations on Virtual Assets

The Financial Action Task Force (FATF) in June 2019 plans to finalize new global standards[1] that aim to ramp up AML/CFT regulation of virtual asset markets, part of a global wave of heightening regulatory expectations for virtual asset transactions. If FATF adopts the proposed standard, jurisdictions would need to require cryptocurrency exchanges to identify and record parties to virtual asset transactions just as other financial institutions do with wire transfers.

- In a February 2019 draft update to Interpretive Note for Recommendation 15 on new technologies,[2] FATF specified that jurisdictions should apply all relevant FATF standards to virtual asset service providers (VASPs), including applying the "travel rule" to transactions worth more than USD/EUR 1,000 and following standards for wire transfers. FATF requested private sector comments focused on the travel rule proposal.
- The update in theory would bring virtual asset transactions in line with travel rule requirements, but virtual asset transfers currently do not always involve third-party VASPs on both ends of the transaction.

The Travel Rule

The travel rule is a foundational element of the global AML/CFT framework. It requires that all financial institutions in a payment chain include and preserve information about the originator and beneficiary on payment messages, so that information about the parties to a payment is available to all financial institutions involved in the payment and to government authorities in each jurisdiction where a payment is processed.

Section 7(b) of the draft interpretive note states that "[c]ountries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to beneficiary VASPs and counterparts (if any), and make it available on request to appropriate authorities."

The practical and immediate impacts of FATF's virtual assets proposal will depend largely on how closely the final version in June mirrors the proposed version, especially in section 7(b). Implementing the travel rule would require VASPs to make significant operational and infrastructure changes, and applying the travel rule to virtual asset transactions would fundamentally alter the nature of many of them.[3] Many VASPs may deem these changes cost-prohibitive.[4] If the Interpretive Note is adopted as-is, the virtual asset industry would likely have to revamp, with many VASPs closing and new types of blockchain platforms would need to be built. The current model for facilitating transfers would be highly unfeasible under the new standards.

- VASPs offer digital wallets that customers use to hold cryptocurrency balances and send amounts to other wallets. Cryptocurrencies run on online distributed ledgers known as blockchains, where transfers can occur between addresses without a regulated intermediary or any intrinsic personal identification of users. Most VASPs that host their customers' digital wallets collect the identification information of their users, but VASPs do not have the technical ability to identify the person behind every possible receiving address on a public blockchain protocol such as Bitcoin that does not have any KYC features.

- For VASPs to identify the users on both ends of a transaction, they might be forced to limit transactions to a defined set of addresses that are affiliated with the VASP, introduce an ID-verification process to allow transactions with external digital wallets, or only offer cryptocurrencies that are built with an additional layer of AML/KYC features, which exist but have minimal market share.[5] Any of these changes would be significant shifts to VASPs' current business model and would severely narrow consumer options for quick peer-to-peer cryptocurrency payments.

- The proposed FATF Interpretive Note could have major implications for financial privacy. Although banks in a payment chain see the names of the beneficiaries of wire transfers, they do not automatically know the balances of any external accounts. In contrast, with most cryptocurrencies, once an address is known, anyone can see the balance of that address. If personal IDs are attached to digital wallet transactions, an individual's cryptocurrency wealth could be known to any receiving VASP, creating immense responsibilities and risks around data privacy.

FATF's virtual assets proposal is part of a broader wave of increased regulation of the cryptocurrency industry. U.S. authorities in particular are aggressively acting against virtual asset businesses running afoul of financial regulations, and the U.S. Treasury Department now adds cryptocurrency addresses to the SDN list.[6] Other jurisdictions also are adjusting their approaches to regulating virtual assets.

- FinCEN in early May published guidance affirming its regulatory framework over virtual currencies and released an advisory to highlight typologies of illicit virtual currency use.[7] The guidance elaborates on the various types of virtual currency activities defined as money transmission and reinforces the applicability of Bank Secrecy Act obligations and the travel rule to VASPs.[8] Treasury's Undersecretary for Terrorism and Financial Intelligence a few days later spoke before a major cryptocurrency industry conference and stressed the need for firms to comply with OFAC sanctions.[9]

- The G-20 in April 2019 announced that central bank governors and finance ministers would meet in early June to discuss ways to increase transparency in the virtual asset sector and combat money laundering and terrorist financing.[10] The results are expected to largely reflect the FATF proposal because G-20 Leaders in 2018 committed to regulate virtual assets at the national level in line with FATF's standards.[11] The U.S. currently holds the FATF presidency and has prioritized clarifying global AML standards for virtual currencies as a key objective for 2018-2019.[12]

- In recent weeks, U.S. and state officials have acted against multiple bad actors in the virtual asset space. FinCEN in late April fined an individual for operating an unregistered peer-to-peer virtual money exchange business that processed $5 million worth of Bitcoin and failed to create any sort of AML program.[13] The U.S. Department of Justice (DOJ) subsequently indicted the owners of a company operating a shadow banking service to serve cryptocurrency businesses that could not open up accounts at financial institutions.[14] Also in late April, the Manhattan District Attorney's office won convictions of two men who were running a darknet drug site and laundering $2.8 million in Bitcoin between 2013 and 2018.[15]

- In late April, the U.S. Securities and Exchange Commission and the U.S. Commodities Futures Trading Commission issued a joint statement warning investors about cryptocurrency scams,[16] noting that the DOJ had recently indicted two Nigerian nationals for defrauding victims out of hundreds of thousands of dollars in Bitcoin.[17]

- Some nations are developing special economic zones[18] and regulatory regimes and sandboxes[19] to promote cryptocurrency businesses, even as the U.S., Canada,[20] and China[21] are cracking down on Initial Coin Offerings (ICOs) within their jurisdictions. The Philippines' Cagayan Economic Zone Authority offers tax incentives to lure virtual currency businesses, and even foreign firms to operate cryptocurrency mining, exchanges, and other services.[22] Zug, Switzerland, has fashioned itself as a "Crypto Valley," with the local government, startups, legal services, and accounting firms catering to domestic and international blockchain ventures.[23] Malta and Bermuda[24] have passed laws to make it easier for companies to conduct ICOs to distribute new digital tokens.

If the virtual asset proposal is adopted without change, the updated FATF standards would face serious hurdles in curbing illicit activity, even if VASPs set up procedures to comply with the travel rule. Most of these hurdles come from the technical features of cryptocurrencies and the ease with which illicit actors can operate using blockchain software.

- There is no practical way for law enforcement to stop the generation of cryptocurrency addresses and the use of non-custodial wallets that fall outside of the FATF standard. Cryptocurrency addresses and non-custodial wallets that fall outside the VASP standard can be created easily with free software.[25] As a result, while VASP services may facilitate fewer illicit transactions, illegal activity is likely to move to still-unregulated platforms.

- In January, the Palestinian terrorist group Hamas started a Bitcoin crowdfunding campaign[26] that initially collected donations using a digital wallet at a major U.S. cryptocurrency exchange.[27] It appears, however, that Hamas realized this left them exposed to U.S. law enforcement and the group later began using more complicated wallet software[28] that probably did not involve a third-party platform.[29]

- In November 2018, U.S. Treasury sanctioned the Bitcoin addresses of two Iranians running cryptocurrency exchange services that processed ransomware funds. Later, one of the sanctioned individuals told the *New York Times* that he simply created a new Bitcoin address a week later and was up and running with a different website.[30]

- Many cryptocurrency enthusiasts are drawn to the peer-to-peer, yet pseudonymous nature of payment systems like Bitcoin. The exchanges serving these customers are unlikely to move easily toward end-to-end identity verification.

- FATF and member jurisdictions may also face the problem of ambiguity and the absence of a well-defined scope for the definitions of "virtual assets" and "virtual asset service providers." The digital currency space is still nascent with many new types of architecture, products, and services developing and there is still considerable uncertainty of whether certain elements fit within proposed definitions. FATF, Financial Intelligence Units (FIUs), and industry may benefit from ongoing consultations to define these terms more precisely as virtual asset markets mature.

Although industry reaction to FATF's proposal has been relatively muted, virtual asset firms are vigorously engaging FATF members behind the scenes. Several companies sent representatives to FATF's private sector consultative forum in Vienna in early May.[31] VASPs most likely have been silent publicly because they are concerned that drawing attention to the changes could cause customers to move away from their services. However, digital assets industry groups have provided formal feedback to FATF.

- Chainalysis, a major blockchain analysis firm, delivered an open letter to FATF arguing that the interpretive note would force "onerous investment and friction onto regulated VASPs."[32]

- Global Digital Finance, a digital asset industry advocacy nonprofit, sent a public statement to FATF outlining how the new rules could be circumvented due to the ease of creating new non-custodial digital wallets.[33] Global Digital Finance also recommended that FATF consider supporting new blockchain technology tools that could help with AML/KYC needs and encouraging procedures for data sharing among FIUs.

When FATF unveils the final standard in June, regulators are likely to increase their expectations for VASPs, particularly if they have not already done so. Virtual asset companies should prepare for heightened regulatory expectations and more scrutiny from their industry peers.

- *VASPs should use blockchain analysis and forensics tools to identify and flag transfers involving known illicit addresses as well as to determine any patterns of illicit activity.* Cryptocurrency data analytics firms like Elliptic, Chainalysis, Cipher Trace, and others provide such tools;[34]

- *Invest in new capabilities and products that would add KYC elements into transfers outside VASP platforms.* Applying the travel rule to all VASP transfers would require VASPs to develop technical solutions to ensure they only interact with compliant wallets. Research and development, as well as industry collaboration will be needed to participate in a more regulated, and less anonymous virtual currency ecosystem.

- *Increase their staff expertise on AML issues.* Many cryptocurrency startups focus more on tax, fraud, and securities compliance because those regulatory issues may appear as more pressing to their business operations than AML or sanctions-related risks. Also, the media's longstanding association of cryptocurrencies with illegal drug markets has made many in the industry overly defensive toward money-laundering accusations. For VASPs to be successful, they will need to hire and retain personnel who take AML threats seriously and are vigilant about shaping a comprehensive culture of compliance; and

- *Engage regulators and law enforcement.* VASPs cannot expect governments to develop suitable regulatory and enforcement frameworks if financial authorities do not understand the technology and markets surrounding virtual assets. VASPs should consistently meet with regulators and support public-private partnerships that foster communication between authorities and industry.

More broadly, financial authorities must prepare to oversee a more mature virtual assets sector, where there is likely to be expansion in both regulated and unregulated activities.

- Research on cryptocurrency transaction data shows that FinCEN's early guidance on virtual currencies in 2013[35] led to lower percentages of illicit activity on U.S. VASPs compared to in Europe,[36] where the EU provided little regulatory guidance until recently.

- There is rising interest in virtual assets from institutional investors that can only be supported by a corresponding increase in legal safeguards and regulators' familiarity with these products and services.[37] Despite the price volatility, consumer interest also persists.[38] With FATF setting clear international standards for jurisdictions to follow, a cleaner, more regulated virtual asset space appears inevitable.

However, the growth of regulated VASPs and AML-compliant users will undoubtedly lead to a virtual asset underground market that continues to provide anonymity and noncompliant transactions.[39]

- Financial officials should expect to encounter two virtual asset ecosystems in which they will need to do the following: (1) work with VASPs to manage risks within the regulated space and (2) use financial intelligence and law enforcement methods to deter financial activities that cross into the illicit and unregulated space.

- To counter illicit finance in the growing virtual asset sector, regulators will need to coordinate internationally. Financial authorities should consider developing joint virtual asset analytic centers to facilitate quicker intelligence sharing on digital currencies. As FATF lays the groundwork for a common set of expectations for AML and sanctions standards applied to virtual assets, members should start planning for ways to implement enforcement mechanisms that consider the technology's inherently borderless nature.

Endnotes

1 Financial Action Task Force, "The FATF Recommendations," 2012 [Updated Oct. 2018], http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

2 Financial Action Task Force, "Public Statement – Mitigating Risks from Virtual Assets," 22 Feb. 2019, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html.

3 Fanusie, Yaya, "Crypto Is About To Look More Like Your Bank," 22 March 2019, https://www.forbes.com/sites/yayafanusie/2019/03/22/crypto-is-about-to-look-more-like-your-bank/#57fcde155630.

4 De, Nikhilesh, "'Onerous' FATF Recommendations Harmful for Crypto Transparency: Chainalysis," 12 April 2019, https://www.coindesk.com/chainalysis-onerous-fatf-recommendations-harmful-for-crypto-transparency.

5 Silcoff, Bruce, "There's a Huge Opportunity for Everyone in Crypto, It's Called KYC/AML," 16 Aug. 2018, https://www.coindesk.com/theres-a-huge-opportunity-for-everyone-in-crypto-its-called-kyc-aml.

6 Fanusie, Yaya and Logan, Trevor, "Treasury Designates Iran-based Digital Currency Exchangers Involved in Ransomware Scheme," 30. Nov. 3018, https://www.fdd.org/analysis/2018/11/30/treasury-designates-iran-based-digital-currency-exchangers-involved-in-ransomware-scheme/.

7 Financial Crimes Enforcement Network, "New FinCEN Guidance Affirms Its Longstanding Regulatory Framework for Virtual Currencies and a New FinCEN Advisory Warns of Threats Posed by Virtual Currency Misuse," 9 May 2019, https://www.fincen.gov/news/news-releases/new-fincen-guidance-affirms-its-longstanding-regulatory-framework-virtual.

8 Financial Crimes Enforcement Network, "FinCEN Guidance," 09 May 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

9 U.S. Department of Treasury, "Remarks of Sigal Mandelker, Under Secretary for Terrorism and Financial Intelligence," 13 May 2019, https://home.treasury.gov/news/press-releases/sm687.

10 Zmudzinski, Adrian, "G20 to Establish Crypto AML and Counter-Terrorism Financing Regulations in June: Report," 07 April 2019, https://cointelegraph.com/news/g20-to-establish-crypto-aml-and-counter-terrorism-financing-regulations-in-june-report.

11 Aki, Jimmy, "G20 Countries to Regulate Cryptocurrencies in Line with FATF Standards," 12 March 2018, https://www.ccn.com/g20-countries-to-regulate-cryptocurrencies-in-line-with-fatf-standards.

12 Financial Action Task Force, "OBJECTIVES FOR FATF – XXX (2018-2019)," 2018, https://www.fatf-gafi.org/media/fatf/content/images/Objectives-FATF-XXX-(2018-2019).pdf.

13 Financial Crimes Enforcement Network, "FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws," 18 April 2019, https://www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money.

14 The United States Attorney's Office Southern District of New York, "Arizona Man And Israeli Woman Charged In Connection With Providing Shadow Banking Services To Cryptocurrency Exchanges," 30 April 2019, https://www.justice.gov/usao-sdny/pr/arizona-man-and-israeli-woman-charged-connection-providing-shadow-banking-services

15 Manhattan District Attorney's Office, "DA Vance Announces Guilty Pleas in $2.8 Million Internet Drug Ring," 23 April 2019, https://www.manhattanda.org/da-vance-announces-guilty-pleas-in-2-8-million-internet-drug-ring/.

16 Investor.gov, "Investor Alert: Watch Out for Fraudulent Digital Asset and "Crypto" Trading Websites," 24 April 2019, https://www.investor.gov/additional-resources/news-alerts/investor-alerts/investor-alert-watch-out-fraudulent-digital-asset.

17 U.S. Attorney's Office District of Oregon, "Two Nigerian Nationals Indicted in Bitcoin Fraud Scheme," 24 April 2019, https://www.justice.gov/usao-or/pr/two-nigerian-nationals-indicted-bitcoin-fraud-scheme.

18 Alexandre, Ana, "Philippine Special Economic Zone Grants Licenses to Three Crypto Exchanges," 11 July 2018, https://cointelegraph.com/news/philippine-special-economic-zone-grants-licenses-to-three-crypto-exchanges.

19 Tassev, Lubomir, "Russia Prepares to Test Cryptocurrencies in Four of Its Regions," 27 April 2019, https://news.bitcoin.com/russia-prepares-to-test-cryptocurrencies-in-four-of-

its-regions/.

20 Rubin, Gabriel, “State and Provincial Regulators in U.S. and Canada Target Initial Coin Offerings,” 21 May 2018, https://www.wsj.com/articles/state-and-provincial-regulators-in-u-s-and-canada-target-initial-coin-offerings-1526918512.

21 BBC, “China bans initial coin offerings calling them ‘illegal fundraising’,” 5 Sept 2017, https://www.bbc.com/news/business-41157249.

22 Morales, Neil Jerome, “Philippines to allow cryptocurrency operators in economic zone,” 25 April 2018, https://www.reuters.com/article/uk-crypto-currencies-philippines/philippines-to-allow-cryptocurrency-operators-in-economic-zone-idUSKBN1HW1KY.

23 Williams-Grut, Oscar, “Here’s what it’s like to visit ‘Crypto Valley’ — Switzerland’s picturesque blockchain version of Silicon Valley,” 02 July 2018, https://www.businessinsider.com/what-its-like-in-zug-switzerlands-crypto-valley-2018-6

24 Popper, Nathaniel, “Have a Cryptocurrency Company? Bermuda, Malta or Gibraltar Wants You,” 29 July 2018, https://www.nytimes.com/2018/07/29/technology/cryptocurrency-bermuda-malta-gibraltar.html.

25 Fanusie, Yaya, “Crypto Is About To Look More Like Your Bank,” 22 March 2019, https://www.forbes.com/sites/yayafanusie/2019/03/22/crypto-is-about-to-look-more-like-your-bank/#57fcde155630.

26 Fanusie, Yaya, “Hamas Military Wing Crowdfunding Bitcoin,” 4 Feb. 2019, https://www.forbes.com/sites/yayafanusie/2019/02/04/hamas-military-wing-crowdfunding-bitcoin/#d9a9f304d7fb.

27 Cuen, Leigh, “Blockchain Analysis Links Hamas Fundraising to Coinbase Bitcoin Account,” 7 Feb. 2019, https://www.coindesk.com/hamas-coinbase-bitcoin.

28 Wilson, Tom and Williams, Dan, “Hamas shifts tactics in bitcoin fundraising, highlighting crypto risks: research,” 26 April 2019, https://www.reuters.com/article/us-crypto-currencies-hamas/hamas-shifts-tactics-in-bitcoin-fundraising-highlighting-crypto-risks-research-idUSKCN1S20FA

29 Fanusie, Yaya, “Jihadists Upping Their Bitcoin Game,” 29 March 2019, https://www.forbes.com/sites/yayafanusie/2019/03/29/jihadists-upping-their-bitcoin-game/#562fdca179bc

30 Erdbrink, Thomas, “How Bitcoin Could Help Iran Undermine US Sanctions,” https://www.nytimes.com/2019/01/29/world/middleeast/bitcoin-iran-sanctions.html.

31 Financial Action Task Force, “Calendar,” https://www.fatf-gafi.org/media/fatf/content/images/Objectives-FATF-XXX-(2018-2019).pdf.

32 Levin, Jonathan and Spiro Jesse, “Email,” 08 April 2019, http://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis_Input_7b_Public_Statement.pdf?mkt_tok=eyJpIjoiWW1abU1HVTFO-VFpsT0RrdyIsInQiOiIyRUlOcHE1c3NOTE-hWRzArVW9uVWw4OGdTUStYTXNDNVNRaz-RkTHFhMFBNMFpjbmNyRW1ha25uclpIVms-0RUNKdlwvTlZ0bWxFOGVoWDN1OHhPZm-9mdTVPQjJmb2JHR09BRzFaR1UxNHU2dFhG-dEQ4bUltZFh1UnJlMEJFYXErck0ifQ%3D%3D

33 Global Digital Finance, “Email,” 07 April 2019, https://www.gdf.io/wp-content/uploads/2018/01/GDF-Input-to-the-FATF-public-statement-of-22-Feb-2019-FINAL.pdf.

34 Roberts, John Jeff, “To Catch a Bitcoin Thief, Call These Detectives,” 27 June 2018, http://fortune.com/2018/06/27/bitcoin-detective-zcash-cryptocurrency/.

35 Financial Action Task Force, “FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities,” 18 March 2013, https://www.fincen.gov/news/news-releases/fincen-issues-guidance-virtual-currencies-and-regulatory-responsibilities.

36 Fanusie, Yaya J. and Robinson, Tom, “Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services,” 12 Jan. 2018, https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf.

37 Bain, Benjamin and Leising, Matthew, “ICE’s Bakkt Has Issues. A N.Y. Crypto License Might Fix Them,” 18 April 2019, https://www.bloomberg.com/news/articles/2019-04-18/bitcoin-going-mainstream-might-hinge-on-new-york-crypto-license.

38 Russolillo, Steven, “Bitcoin Surges Above $8,000; Investors Say ‘Crypto Winter’ Is Over,” 14 May 2019, https://www.wsj.com/articles/bitcoin-surges-above-8-000-investors-say-crypto-winter-is-over-11557818848.

39 Fanusie, Yaya, “Good Crypto, Bad Crypto: Blockchain Projects Gaining Legitimacy While Spawning An Underground,” 12 July 2018, https://www.forbes.com/sites/yayafanusie/2018/07/12/good-crypto-to-bad-crypto-blockchain-projects-gaining-legitimacy-while-spawning-an-underground/#31b86dc31078.