ELLIPTIC ADVISORY

June 27, 2019

THE FATF'S UPDATED GUIDANCE ON VIRTUAL ASSETS

Summary

On June 21, 2019, the Financial Action Task Force (FATF), the global standard-setter for anti-money laundering and countering the financing of terrorism (AML/CFT) regulation, released guidance on virtual assets, which include cryptocurrencies and other digital payment methods (*Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers)*[1]. The newly-released document updates the FATF's earlier guidance on the sector issued in 2015.[2]

The FATF's new guidance aims to assist regulators, Virtual Asset Service Providers (VASPs, a term that includes cryptocurrency exchanges, custodial wallet providers, etc.), and other financial institutions (FIs) in applying global AML/CFT standards as they relate to virtual assets. Of particular relevance to Elliptic and its customers are sections of the FATF's new guidance describing:

- the importance of transaction monitoring solutions;
- the importance of conducting a firm-wide risk assessment;
- the global requirement to implement FATF Recommendation 16 (the "Travel Rule");
- the application of the FATF standards to a wide range of product and service providers;
- the importance of address blacklisting and typologies development; and
- the need for banks to develop a risk-based approach to virtual assets.

The FATF has allowed for a one year period during which it will monitor how both the public and private sectors are implementing its updated standards. As a result, cryptocurrency exchanges and other VASPs can expect to face significant scrutiny from local and global regulators until June 2020.

[1] See the FATF's 2019 *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* here: http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

[2] See the FATF's June 2015, *Guidance for a Risk Based Approach: Virtual Currencies,* here: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

Below is a detailed analysis of certain key features of the FATF's new guidance and their relevance for users of Elliptic's product and service offerings.

Contact us to learn more about how we can assist your business in addressing specific issues covered in the FATF's new guidance.

Analysis and Key Takeaways

1) The FATF's guidance indicates that transaction monitoring solutions are essential for effectively managing risks related to virtual assets.

Recently, regulators have begun to recognize the importance of automated transaction monitoring solutions as a pillar of AML compliance in the crypto space.

For example, in its May 2019 guidance, the US Financial Crimes Enforcement Network (FINCEN) noted that crypto businesses can comply with their AML obligations by relying on solutions "to track and monitor the transaction history of a [cryptocurrency] through publicly visible ledgers."[3] Regulators in Hong Kong and Abu Dhabi have also set out their expectations that crypto businesses should deploy transaction monitoring solutions to identify activity associated with tainted addresses.[4]

The FATF's new guidance now enshrines the importance of transaction monitoring as a pillar of effective AML/CFT risk management for the sector. This marks a significant step in setting global expectations regarding monitoring practices for cryptocurrencies and other virtual assets. At Elliptic, we previously called on the FATF to clarify the role of transaction monitoring for the sector, so we welcome this new clarity.

According to the FATF, "VASPs . . . should have the ability to flag for further analysis any unusual or suspicious movements of funds or transactions . . . indicative of potential involvement in illicit activity . . ."[5]

[3] See FinCEN Guidance, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," May 9, 2019, p. 21, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

[4] See Securities and Futures Commission of Hong Kong, "Conceptual Framework for the potential regulation of virtual asset trading platform operators," November 1, 2018, pp. 6 - 7, https://www.sfc.hk/web/EN/files/ER/PDF/App%202_%20Conceptual%20framework%20for%20VA%20trading%20platform_eng.pdf; See Abu Dhabi Global Market Financial Services and Regulatory Authority, "Guidance - Regulation of Crypto Asset Activities in the ADGM", May 14, 2019, pp. 23, 30 - 31. http://adgm.complinet.com/net_file_store/new_rulebooks/g/u/Guidance_Regulation_of_Crypto_Asset_Activities_in_ADGM_140519.pdf

[5] See the FATF's June 2019 guidance, p. 44.

The FATF's guidance also notes that, "Monitoring should be carried out on a continuous basis . . . Where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring . . ."[6]

The FATF further emphasizes that monitoring should be risk-based, with attention focused on higher risk activities. According to the FATF, "VASPs . . . should adjust the extent and depth of their monitoring in line with their institutional risk assessment and individual customer risk profiles."[7] The FATF also emphasises that VASPs should have clearly established and documented parameters for determining the allocation of risk levels when monitoring customer activity.[8]

Elliptic's AML monitoring software enables crypto businesses to engage in ongoing transaction monitoring at scale. It is an essential component of effective AML/CFT risk management for cryptocurrency exchanges and other regulated actors in the sector. Elliptic's customizable AML risk rules allow our customers to adjust monitoring parameters to their needs, in alignment with regulatory expectations, so that they can direct their compliance resources to scrutinizing the key risks their business faces.

Elliptic's Professional Services and Customer Services teams can assist our customers in the implementation of AML risk rules suited to their specific transaction monitoring needs. Contact us to learn more.

2) The FATF regards a risk assessment as a central feature of any VASP's AML/CFT framework.

FATF Recommendation 1 underscores the importance of conducting a risk assessment as the foundation of a risk-based approach "to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified."[9]

The FATF's new virtual asset guidance indicates that all VASPs should be required by their local regulators to conduct a risk assessment that they can use to design controls for countering financial crime risks.

According to the FATF, "A VASP's risk assessment should take into account . . . the types of services, products, or transactions involved; customer risk; geographical factors; and type(s) of [virtual asset] exchanged, among other factors."[10]

---

[6] Ibid., p. 42.
[7] Ibid., p. 42.
[8] Ibid., p. 42.
[9] See the FATF Recommendations, p.9, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, p. 9.
[10] See the FATF's June 2019 guidance, p. 11.

The FATF further notes that the outcomes of this risk assessment should inform a VASP's transaction monitoring practices. It states that VASPs "should adjust the extent and depth of their monitoring in line with their institutional risk assessment and individual customer risk profiles. . . . Monitoring under a risk-based approach allows [a crypto business] to create monetary or other thresholds to determine which activities will be reviewed . . . VASPs should document and state clearly the criteria and parameters used for customer segmentation and for the allocation of a risk level for each of [its] clusters of customers, where applicable."[11]

Elliptic's Professional Services team assists our customers in conducting risk assessment exercises as a basis for calibrating our AML risk rules, as well as the design of other critical AML/CFT controls. Contact us for more information on, and assistance with, designing and executing an effective risk assessment to inform your AML/CFT compliance program.

3) The FATF has made the "Travel Rule" a formal global requirement. VASPs must be able to distinguish between those transactions that involve other regulated financial institutions, and those that do not.

The FATF's new measures require for the first time that all VASPs must comply with FATF Recommendation 16. This sets out that VASPs must obtain, hold, and transmit required originator and beneficiary information related to funds transfers involving other VASPs or regulated financial institutions (known as the "Travel Rule").

Going forward, when facilitating a transaction on behalf of a customer, originating VASPs must obtain and submit to any recipient VASP or regulated financial institution, the following information:

(i) the originating customer's name;
(ii) the originating customer's wallet number;
(iii) the originating customer's address and identifying information;
(iv) the beneficiary customer's name;
(v) the beneficiary's wallet number.[12]

Both the originating and recipient VASPs must retain the relevant information and make it available to law enforcement on request. VASPs must therefore have solutions in place for enabling them to obtain, hold, and transmit this information.[13]

The FATF's June guidance clarifies, however, that this end-to-end recordkeeping and data transmission requirement only applies where an originating VASP's customer is sending funds to a counterpart at another VASP or regulated business. It would not apply in other circumstances, such as in purely peer-to-peer (P2P) transactions, where a regulated entity is not involved.

[11] Ibid,. p. 42.
[12] Ibid., p. 29.
[13] Ibid., p. 43.

For example, a cryptocurrency exchange's customer may send funds from their exchange-hosted wallet to a non-custodial address that is not part of another VASP's cluster of addresses. According to the FATF, in these situations, the originating VASP must still collect and retain information on its own customer (i.e. the sender). But, it does not have any obligation to obtain or transmit beneficiary information since there is no VASP or other regulated business on the other end of the transaction to receive the required information.

Conversely, a VASP whose customer receives inbound funds from a non-custodial address must still ask its customer about the identity of the sender and must retain that information so that it may be provided to law enforcement upon request.[14]

Elliptic's Customer Engagement team works with our customers to understand compliance challenges they face related to the Travel Rule. Our AML software can assist our users in identifying if their own customers' outbound transactions involve cryptocurrency addresses that are associated with another VASP's cluster of addresses and would therefore be subject to the Travel Rule's recordkeeping, transmission, and reporting requirements.

Similarly, our solution can assist our users in identifying transactions that involve outbound transfers to non-custodial addresses that are not associated with VASPs, and where there would not be a requirement to transmit full sender and beneficiary information. Recipient VASPs can also utilize our AML tool to verify customer's claims about the source of inbound funds transfers.

Contact us to learn more about these measures and to discuss your company's response to the Travel Rule.

4) The FATF's new standards apply to a wide range of virtual asset products and services. Service providers across the sector need to understand their requirements, and must ensure comprehensive compliance.

The FATF's 2015 guidance suggested that countries should focus their attention on the regulation of fiat-to-virtual asset exchange platforms, but said little about regulatory treatment of other product and service types.

The FATF's new measures now apply to a broad range of emerging service providers, such as virtual asset-to-virtual asset (or "crypto-to-crypto") exchange platforms, issuers of initial coin offerings (ICOs). bitcoin ATMs, custodial wallet providers, brokerage services, and a range of other platforms and services that facilitate virtual asset transfers.[15]

[14] Ibid., p. 30.
[15] Ibid., pp. 13 - 15.

The FATF guidance also addresses specific circumstances under which P2P trading platforms, decentralized exchanges (DEXs), and decentralized applications (Dapps) may be covered by regulation. Namely, where they are more than a passive platform for enabling users to conduct trades but instead actively facilitate customer trades and exchange.[16]

The FATF's message is clear: a broad set of platforms and services providers can fall within the definition of a VASP and are subject to AML/CFT requirements.

Elliptic has extensive working with VASPs of all stripes - such as bitcoin ATMs, ICO issuers, and beyond - to develop innovative compliance solutions that meet their specific requirements. Contact us to learn more about the range of compliance services we offer that can assist your business in complying with AML/CFT regulation.

5) The FATF stresses that data sharing and typologies development are critical for assisting in the identification and management of risks.

Solutions like those we've pioneered at Elliptic make it possible for VASPs to identity cryptocurrency addresses associated with specific illicit actors, such as dark web marketplaces, sanctioned actors, and terrorist financiers.

The FATF guidance endorses the practice of VASPs developing blacklists of suspicious and high risk addresses, and sharing those lists with others.

According to the FATF, "If a VASP uncovers addresses . . . that it has decided not to establish or continue business relations with or transaction with due to suspicions . . . the VASP should consider making available its list of 'blacklisted wallet addresses' . . ."[17]

The FATF's guidance also encourages the public and private sectors to share information on risks in the virtual asset space, including through the development and sharing of "typologies and methodologies of how money launderers or terrorist financiers misuse VASPs . . ."[18]

At Elliptic, we've enabled our customers to share with us information on suspicious cryptocurrency addresses that we incorporate into our AML tool, making those high risk addresses visible to our other users - enhancing their ability to detect suspicious transactions. For example, in May 2019, we announced a data-sharing partnership with our customer Wirex to allow it to share with us addresses associated with confirmed fraud, for incorporation into our AML tool.[19]

[16] Ibid., pp. 15 - 16.
[17] Ibid, page 41.
[18] Ibid, page 39.
[19] See Elliptic press release, "Wirex and Elliptic unite in new approach to make cryptocurrency safer," May 23, 2019, https://www.elliptic.co/press-releases/wirex-elliptic-unite-cryptocurrency-safer

We've also published a comprehensive typologies report with detailed money laundering and terrorist financing red flags specific to the crypto space, providing our customers with information they can use to strengthen their compliance controls. Contact us to receive more information about our data sharing and typologies development initiatives.

6) The FATF indicates that banks should not de-risk the virtual asset sector but should adopt a risk-based approach instead for managing relationships with VASPs.

To date, many banks and FIs have attempted to avoid risk exposure by simply de-risking and avoiding all contact with crypto exchanges and other VASPs. As a result, many VASPs have struggled to obtain, or maintain, banking relationships.[20]

However, the FATF's new guidance makes clear this situation is neither desirable nor sustainable.

The FATF's guidance indicates that banks and other FIs "that provide banking services to VASPs or to customers involved in [virtual asset] activities . . . should apply a risk-based approach when considering establishing or continuing relationships with VASPs or customers involved in VA [virtual asset] activities, evaluate the ML/TF risks of the business relationship, and assess whether those risks can be appropriately mitigated and managed."[21]

The FATF also notes that flat-out de-risking is not an appropriate response. It states that, "the FATF does not support the wholesale termination or restriction of business relationships with a particular sector (e.g. FI relationships with VASPs, where relevant) to avoid, rather than manage, risk in line with the FATF's risk-based approach."[22]

At Elliptic, our Professional Services team works with banks and other FIs to develop strategies and solutions for managing risks related to the virtual asset sector. We assist FIs to develop thoughtful, risk-based measures that allow them to identify and assess their exposure to cryptocurrency-related risks and to design bespoke solutions for mitigating those identified risks.

Contact us to learn more about our services for banks and other FIs seeking to apply a risk-based approach for dealing with cryptocurrency exchanges and other virtual asset-related activities.

[20] See for example, Martin Arnold, "Cryptocurrency companies forced to bank outside the UK," Financial Times, 23 October 2017, https://www.ft.com/content/3853358e-b508-11e7-a398-73d59db9e399
[21] Ibid., page 8.
[22] Ibid.,, page 11.