MONERO

Monero Policy Working Group (MPWG)
Date: 2021-04-19

Response to the Financial Action Task Force (FATF) updated Guidance for a risk-based approach to virtual assets and VASPs

Submitted by: Monero Policy Working Group
Authors: Dr. F. X. Cabañas; Dr. J. Dubois-Lacoste; Justin Ehrenhofer;
Deanna MacDonald; William Miller; Dr. R. Renwick; Asst. Prof. Dr. A.J. Santos.

Contact: policy@getmonero.org

Introduction

1. The Monero Policy Working Group (MPWG) is a loosely formed quorum of individuals that contribute to the Monero[1] open-source project. Monero is a permissionless, privacy-preserving cryptocurrency network. The goal of MPWG is to work with regulators, policy makers, and the wider financial services sector to communicate broad understanding of Monero, and other privacy-preserving cryptocurrencies. We have specific interest in interacting with entities, so they may understand Monero's component technologies, especially with regards to evolving regulatory framework and compliance requirements. We thank you for the opportunity to respond to the *Draft updated Guidance for a risk-based approach to virtual assets and VASPs*, and applaud the efforts towards transparency in the drafting process. We give consent for our contribution to be publicly published in full, and welcome any questions you may have on the content of our response.

2. We would like to first state that we find the proposed guidelines as lacking in brevity, cohesiveness, and clarity, even if we offer sympathy to the difficulties of reaching consensus in multi-stakeholder environments, and understand the complexity that comes with overarching 'political imperatives.' The proposed document is supposed to aid understanding and provide certainty to regulatory bodies, however we feel it falls short - confusing the reader by being overly accommodating (and even recommending) arbitrary interpretations by nations.

3. **Our primary concern is that the proposed guidelines explicitly encourage broad interpretation of the provided definition of both VAs and VASPs.** Encouraging broad interpretation will not aid in regulatory harmonisation or certainty. It will likely cause the opposite effect: jurisdictions will inevitably implement differing regulations as they seek legitimacy for their interpretations of perceived risks and what risk based approaches to VA and VASPS should mean, including the intention of providing a favourable investment

[1] *see* The Monero Project, https://github.com/monero-project and https://getmonero.org.

environment. Such broad interpretation often comes at the expense of an integrative approach and thus global system integrity.

4. Considering this, we feel these guidelines do not aid in risk-related regulatory decision making, but merely accommodate further regulatory arbitrage, as jurisdictions seek to foster continued national investment, foreign direct investment, and innovation in the sector through regulatory uncoupling, tax incentives, and promotion of financial ecosystems conducive to experimentation - including ones that will continue to pose considerable ML/TF risk.

5. We also question some of the proposed 'Recommendations,' which seem to lack any sort of balanced discussion weighing up potential benefits against inherent risks. This is especially worrisome as the lack of proportional, well reasoned, and transparent debate may expose certain legislative bodies and the coupled regulatory entities to political (or even legal) redress.

6. More specifically, we would like to address the following:

    a. The provided definition of VASP requires more in-depth consideration. It seems to state that a VASP may be "any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:...". **We support the need to define what constitutes a VASP, but strongly disagree with recommendations of a broad interpretation. When interpreted broadly, as suggested, we do not feel there is a reasonable or proportional boundary of what constitutes 'non-covered activities'.**
    b. We urge clarity to ensure that jurisdictions acknowledge that the private ownership, use, and interaction with blockchain networks (including validating transactions, interacting with multisig transactions as a minority key holder, as well as methods known as liquidity provision, staking, voting, and algorithmic design) distinctly do not fall under the definition of a VASP.
    c. **We would like to highlight that any movements to include natural persons acting on their own behalf would seem to alter the perceived mandate of the FATF, in a manner best described as 'Scope Creep'.** Acknowledging this would be beneficial, so the public, national bodies, competent authorities, and regulatory bodies are aware of the evolution of the mandate bestowed to an international harmonisation body purported to be tasked with regulating obliged entities, in the traditional sense.

7. Considering the above, we are in support of Paragraph 23. We acknowledge the considerable work undertaken to ensure Guidelines exist to support national bodies in their assessment of risks, and methods for supervisory control in the sector. **We understand the grave danger of laissez-faire oversight, especially considering the relatively recent history of ML/TF activities that have come to light from established (otherwise respected) incumbents who were mistakenly thought to have been**

acting in appropriate manners.[2] Any efforts made to ensure that VAs do not provide another avenue for distinct, and persistent, regulatory abuse should be welcomed by the sector. This is one reason why we stress more strict scoping of the definitions be provided.

8. We welcome the conversation regarding P2P transactions contained within paragraphs 34 and 35. **We also welcome the acknowledgement and clarity that P2P transactions do not fall under the remit of the FATF, nor within the purview of AML/CTF regulations.** We also support functionality to aid regulatory and financial supervision with respect to mitigating ML/TF risks, including techniques such as - but not limited to - transaction view keys and wallet view keys, which enable natural persons to provide requested or subpoenaed information to appropriately trusted bodies (*e.g.*, regulators, custodians, auditors) as appropriate and in conformity with due process safeguards. We feel these technologies provide more certainty to interventions - especially with regards to investigations and audits, as opposed to other techniques, such as transaction analysis, blockchain analytics, or blockchain surveillance.

9. We would like to draw attention to paragraph 36 (e). **We do not (and have yet to see) what 'anonymization functions' (or indeed AECs) are supposed to mean in the context of virtual assets.** Are the FATF attempting to draw attention to privacy-preserving techniques, or to privacy-preserving cryptocurrencies? Clarity on this would be helpful, especially in the light of data protection regulatory frameworks, privacy rights, and information security techniques. The use of a Bitcoin address can be considered an 'anonymization function,' for example. Distinction and guidance on this is necessary, as it would seem that the FATF (and other competent authorities) misrepresent certain privacy-preserving technologies, as being harmful when they are well intentioned from a privacy, data protection, security, and consumer protection perspective - as clearly outlined in the recently published ISO/TR 23244:2020 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations.[3]

10. We appreciate the desire indicated in paragraph 68 to be technology neutral, but are unsure how this may be parsed with elements of the document that seem to suggest that certain technologies pose greater risk than others while at the same time recommending specific technological risk mitigation tools. Clarity on this is welcomed.

11. Paragraph 69 says "The FATF does not seek to regulate as VASPs natural or legal persons that provide ancillary services or products to a VA network." While we generally agree with this sentiment, it is unclear to us what this actually means. Further clarity would be welcomed, especially in the light of the broad interpretations that are urged regarding VASPs. These two provisions do not seem congruent, unless that was the intention?

12. We would like to draw attention to Paragraph 79, which intimates that developers (and potentially node operators if the Guidelines are to be interpreted broadly as suggested) may be designated VASPs - if they launch code that carries out an activity that may be classified as normally being carried out by a VASP. This is discordant, especially in the case a service

[2] https://www.bbc.com/news/uk-54226107

[3] https://www.iso.org/standard/75061.html

is launched as a public utility (as opposed to a profit making venture). It would seem that seeking profit through the actions of business activities is no longer the predominant measure against which VASP classification is determined. This is quite a step change, especially as earlier in the Guidelines, the seeking of profit is stipulated as being an explicit classifier (see Paragraph 68). **It would seem, from our perspective, that the FATF Guidelines now treat public good utilities, as well as profit making exercises, equally. The general public, national bodies, competent authorities and regulators should be made explicitly aware of this change, to improve accountability and transparency.**

13. Regarding paragraph 91 c), e) - caution is urged in suggesting that countries deny licences to VASPs if they allow transactions from/to non-obliged entities (self-custodied/unhosted wallets). **It is the position of this workgroup that it is beneficial for the FATF to encourage countries to embrace P2P transactions and transactions to non-obliged entities, since valuable data points for regulators and law enforcement are obtained through exactly these types of transactions, especially when non-obliged entities come into contact with VASPs that have properly functioning AML and KYC policies and procedures in place.** We urge the FATF to reconsider this wording and intent. Following on from this, we would urge caution when countries are considering prohibiting or limiting certain VA activities. Experience has shown that prohibition has not always achieved the desired result, and in many cases actually achieved the opposite. Legislation having the effect of forcing certain VA activities underground, where a licensed VASP is not party to transactions, will serve to virtually eliminate what limited data points law enforcement already have.

14. We would like to draw specific attention to the information provided concerning investigation tools, especially those deemed blockchain surveillance, otherwise known as ‘blockchain analytics’, ‘chain analysis’, ‘blockchain analysis’, ‘know your transaction (KYT)’, etc... We strongly welcome the clarity that footnote 32 provides, but are unsure why it is a footnote and not deemed suitable for placement in the main body of text. **Probabilistic analysis poses its own risks to the overall effectiveness of an investigative approach to risk assessment and risk appraisal, including raising possible counter-arguments based on plausible deniability. It also links to potential sources of harm, including the possibility of data protection liability at the hands of both the surveillance service providers, and the obliged entities, that utilise such methods.**

15. We welcome the clarity by which this potential liability is pointed to in the text, as provided in Page 3 of the document, Paragraph 96, Paragraph 139 (d), and Paragraph 209. As a policy working group, we strongly urge explicit movements to more fairly balance data protection and privacy obligations with efforts to mitigate ML/TF risks, such as those pointed out in very recent Guidelines produced by the European Commission.[4] This includes the opinion of the European Data Protection Supervisor, Mr. Wojciech Wiewiórowski, quoted as

[4] Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, Version 2.0, Adopted on 15 December 2020, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf

saying: “We welcome the Commission’s commitment to rely on the risk-based approach to streamline the legislative framework for the prevention of money laundering and terrorism financing, in line with the principle of proportionality. **The Commission should strike a balance between the necessary measures to take for the general interest and the goals of the AML/CFT and the respect of the fundamental rights of privacy and personal data protection.** General compliance with the EU AML/CFT rules by Member States must go hand in hand with the GDPR and the data protection framework”.[5]

16. Further to this, caution is urged when advising countries to use ‘blockchain surveillance’ as a risk mitigating measure in Enhanced Due Diligence (EDD). While broad mention of this is made in footnote 32, as discussed above, we believe a more robust cautionary statement to countries on the shortcomings of overreliance of ‘blockchain surveillance’ is warranted. Such shortcomings are illustrated by the following:

    a. There exists a lack of transaction correlation in a significant number of cases. This becomes apparent when there is a single chain of transactions with no other chains of transactions that merge with it. For example: a single chain of transactions originating from a VASP.
    b. Transactions which occur ‘off-ledger’ by the trading or theft of private keys. For example, a scenario where a false positive ‘red flag’ can be associated with an innocent user of cryptocurrency is as follows: An individual has her Bitcoin wallet on a hardware device. It is physically stolen from her office, along with the piece of paper containing her written private key. The thief then uses the Bitcoin from the Bitcoin wallet to purchase a banned item online. Because the theft of the Bitcoins occured off-ledger (the physical device was stolen), ‘blockchain surveillance’ will show the individual who had her Bitcoin wallet stolen as being counterparty to the transaction where the thief purchased the banned item. The individual is implicated in the crime. A more sophisticated example involves the simultaneous exchange, ‘off-ledger’ of private keys representing ‘clean’ Bitcoin and the stolen Bitcoin in the previous example. This allows the thief to launder the stolen Bitcoin. The stolen Bitcoin is then used for more serious criminal activity, by a criminal different from the original thief. The additional value for the other criminal is that, unlike clean Bitcoin, these stolen Bitcoin purchased on the black market cannot be traced back to her. The stolen Bitcoin would instead be traced by a ‘blockchain surveillance’ company to either the victim of the original theft or even to a legitimate customer of the victim of the original theft. The use of ‘blockchain surveillance’ in these, and other similar, scenarios has the negative result of implicating perfectly innocent citizens in criminal or terrorist activity, while at the same time facilitating money laundering and/or terrorist financing.
    c. We believe that those who promote the use of ‘blockchain surveillance’ as the primarily recommended means of mitigating money laundering and/or terrorist

[5] Data Protection requirements must go hand in hand with the prevention of money laundering and terrorism financing, available at: https://edps.europa.eu/press-publications/press-news/press-releases/2020/data-protection-requirements-must-go-hand-hand_en

financing risks must address critical questions regarding the scalability and viability of such methods as the size and utilisation of blockchains increase. 'Blockchain surveillance' can be modelled as the number of ways of choosing K 'dirty' outputs from a set of N total outputs in a blockchain. While the cost of the normal use of a blockchain scales linearly with N, 'blockchain surveillance' scales as the binomial coefficient, N!/(K!*(N-K)!).[6] The question of the scalability of 'blockchain surveillance' as the size of blockchains increase was raised by FinCEN in the United States: "Blockchain analysis can be rendered less effective by a number of factors, including the scale of a blockchain network".[7] It is important to ensure technological neutrality, since changes in technology make larger blockchains more viable, for example, via Nielsen's Law.[8] With this in mind, the question of the scalability of 'blockchain surveillance' will become paramount in time.

d. There are significant adverse effects with the use of 'blockchain surveillance' for profit. In particular, there is a growing tension between 'blockchain surveillance' and both current (European Union; California), and proposed (Canada) data protection, privacy, and consumer protection laws. For example, a major 'blockchain surveillance' company is now marketing surveillance of customers, providing a service to profile consumers and their economic behaviour.[9] The already existing complexity, uncertainty, and ambiguity associated with risk assessment is further perpetuated and, likely inversely affected, by the profit driven motivations of these entities.

e. Innocent members of the social networks of an alleged criminal may be falsely implicated in crimes by way of association. This can occur regardless of when a crime was committed; at some unspecified point in the future or past. An example of this is when an individual engages in illegal activity using cryptocurrency, and then makes a legitimate p2p cryptocurrency transaction one month later with an innocent peer, from the same wallet used previously in a crime. Transaction networks mapped from the offending wallet address would taint innocent individuals, as graph networks drawn from transactions between peers would implicate a host of participants by association.

17. We would like to discuss the process of identification of persons who manage or own a so-called 'unhosted wallet'. **Proving control over an 'unhosted wallet' is possible when using certain privacy-preserving VAs.** It is possible for an individual to demonstrate that they have 'de facto' access and control to the 'unhosted wallet' by one of two methods:

a. The VASP requests the owner of the wallet to sign a message with the declared private key associated with the wallet. This method is already the industry standard in some jurisdictions[10] for popular cryptocurrencies, such as ETH and

[6] https://mathworld.wolfram.com/BinomialCoefficient.html

[7] https://public-inspection.federalregister.gov/2020-28437.pdf, p.12

[8] https://www.nngroup.com/articles/law-of-bandwidth/

[9] https://go.chainalysis.com/business-data-subscription.html

[10] https://www.dukascopy.com/swiss/english/crypto/sign-message

BTC. While this method is, admittedly, not perfect, it goes some way to mitigating the risks that present themselves when VASPs interact with 'unhosted wallets.' This method may also be used for privacy-preserving cryptocurrencies, such as Monero.

b. Alternatively, the VASP may issue a micro deposit to the 'unhosted wallets' public address (or sub-address). This method is only efficable with specific privacy-preserving cryptocurrencies. In Monero the sending address, receiving address, and amounts sent are private (only known to the VASP and the supposed controller of the wallet), so only the holder of that wallet's private key may accurately report back to the VASP the amount and timing of micro deposits received. This is currently done with the verification of traditional banking accounts. While it does not categorically prove ownership (multiple parties may be viewing the wallet's balance), it does get a step closer to demonstrating control, and is potentially more accurate than other proposed methods of wallet control/ownership verification. However, this method is not appropriate for transparent networks, where amounts, sender, recipient, and transaction timestamps are all broadcasted publicly.

18. We would like to draw attention to the advantages of encouraging VASPs to develop appropriate risk mitigation measures in this context, and to embrace privacy-preserving cryptocurrencies rather than discourage or prohibit their use. **In our assessment, it is more beneficial for a jurisdiction to retain data points regarding user deposits and withdrawals of a privacy-preserving cryptocurrency from/to a VASP, rather than to effectively outlaw the use of privacy-preserving cryptocurrencies by encouraging VAPSs to not engage with them.** In a scenario where privacy-preserving cryptocurrencies are effectively outlawed, the code base of these cryptocurrencies does not cease to exist. In such a scenario, it is likely that the use of such cryptocurrencies will be driven underground or to other favourable jurisdictions. Certain privacy-preserving cryptocurrencies (such as Monero) can in fact provide a more robust picture (than 'blockchain surveillance' - see footnote 33 from FATF) of address control, as detailed above.

19. As the guidance makes clear, in numerous places, **relevant authorities should coordinate to ensure required information can be shared ('the Travel Rule') in a manner that is compatible with national data protection and privacy rules.** We strongly appreciate the emphasis on data protection and privacy. We view Travel Rule information sharing as a critical AML measure that must be implemented carefully to ensure that companies comply with strict data protection guidelines, and whilst protecting the privacy and data protection rights of individuals. **It is plainly irresponsible (and potentially negligent) to put personally identifiable information (or other personal data) on a public blockchain, where the consequences of an encryption error (or a leak of a decryption key) would be significant and irreversible.** Further, information held by VASPs for compliance purposes must be protected in accordance with relevant data protection laws.

20. We would like to draw further attention to Paragraph 274 a). In our opinion, the use of privacy-preserving cryptocurrencies should not be a red flag indicator in itself. It is highly likely that as time progresses, more and more VAs will have privacy-preserving characteristics incorporated into them, making them more opaque to outside observation - especially given the numerous risks that are posed from maintaining and using systems that publicly broadcast financial information (price disriminiation, profiling, re-identification, etc). **We urge the FATF to anticipate the increased use of privacy preservation techniques and features in VAs, and issue guidance which encourages countries to develop policies and procedures to interact with and embrace them.**

21. To conclude, we thank you for taking the time to read our response, and are grateful for the transparent manner in which you published the proposed amendments to the Guidelines. As stated, we welcome an inclusive, open, and transparent discussion - preferably in public forums - through which this discussion on the nature of coordinated regulatory effort may take place. Technological innovation often precedes regulation, but that is not to say that regulation, based on common understanding and guiding principles, cannot be conducive to continued technological evolution and innovation - creating harmonious, fruitful relationships between entities that represent public, private, or open-source initiatives. As stated, we are happy for our response to be published publicly, and welcome any questions that you may have. These may be directed at the email provided in the front matter of this response.