GLOBAL
DIGITAL
FINANCE

April 7, 2019

To:
The Financial Action Task Force ("FATF")

Re:
GDF Input to the FATF public statement (the "Public Statement") dated February 22, 2019[1]

Dear FATF Team,

We support efforts by global standard setters, national authorities and regulators to consult and work with the nascent global digital/virtual asset industry.

To that end, we are hereby providing input to the FATF Public Statement dated February 22, 2019 in which the FATF invites private sector entities and other experts to provide written comments on Paragraph 7(b) as regards to the application of Recommendation 16 ("R16") to virtual asset service providers ("VASPs").

The input has been drafted by the GDF AML CFT Working Group, which had also given feedback in a letter dated October 9, 2018[2] and an email dated February 18, 2019.

About GDF

Global Digital Finance ("GDF") is a not-for-profit industry body that promotes the adoption of best practices for crypto and digital assets and digital finance technologies through the development of conduct standards, in a shared engagement forum with market participants, policymakers and regulators.

---

[1] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html

[2] https://www.gdf.io/resources/

Established in 2018, GDF has convened a broad range of industry participants, with 300+ global community members—including some of the most influential digital asset and token companies, academics and professional services firms supporting the industry. GDF is proud to include Circle, ConsenSys, DLA Piper, Diginex, Hogan Lovells and R3 as patron members.

The GDF Code of Conduct is an industry-led initiative driving the creation of global best practices and sound governance policies, informed by close conversations with regulators and developed through open, inclusive working groups of industry participants, legal, regulatory and compliance experts, financial services incumbents and academia. Code principles undergo multiple stages of community peer review and open public consultation prior to ratification.

GDF also conducts policymaker, regulator and industry outreach to build a shared understanding of the risks and opportunities presented by digital assets and tokens. We convene quarterly Summits during which national and regional regulators and supranational policy makers participate as observers.

About the GDF AML/CFT Working Group

The GDF AML/CFT Working Group was established in May 2018, initially to provide input to the FATF ahead of the September 2018 Plenary.

The group now has over seventy members, distributed across the globe, who meet weekly to fulfil the following remit:

1. Respond to consultations, including request for input on the FATF Public Statement discussed in this letter.

2. Develop an AML/CFT Code of Conduct in line with the existing codes developed by the GDF community.

3. Develop best practice guides to support VASPs in creating a baseline industry standards with regards to the detection and prevention of money laundering and terrorist financing.

Summary Inputs

We structure our response to the Public Statement as follows:

1. We provide input on 7(b) explaining that the expectation that "*Countries 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)*" appears to presuppose that an originating VASP has access to other information on the beneficiary apart from the wallet address, which it does not. We also explain that this requirement can easily be circumvented by

interposing peer-to-peer ("P2P") transfers or non-custodial wallets, which cannot be stopped. By implication this requirement potentially has several unintended consequences, including -

a. Encouraging P2P transfers via non-custodial wallets, which are significantly harder for law enforcement to track or control, akin to peer-to-peer cash transfers today.

b. Reducing the prevalence of VASPs, one of the most effective forms of prevention and partnership to law enforcement working in the virtual asset sector.

For these reasons we propose that the underlined be removed.

2. In light of the above, we offer alternative solutions for consideration to 7(b) to neverthless achieve the R16 objectives[3], including:

    a. Definition and enforcement of robust CDD/KYC minimum standards.

    b. Increased emphasis on information sharing, including the use of a global public-private sector sharing initiative, as well as effective use of national sanctions lists.

    c. Use of CDD/KYC consortia and digital identity.

3. To put blockchain—the technology that underpins the growing ecosystem of virtual assets—in a broader context, we provide an overview on the law enforcement benefits of blockchain, alongside how blockchain forensic software tools can aid VASPs and law enforcement in the fight against financial crime.

4. We also provide some thoughts and input on the other sections of the Public Statement on the understanding that these are not subject to consultation.

5. We finish with providing input on Recommendations 10-21 ("R10-21"), as the Public Statement notes that these Recommendations will also apply to VASPs.

[3] These are set out in the Interpretative Note to R.16 as follows:

1. *Recommendation 16 was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and beneficiary of wire transfers is immediately available: (a) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, and prosecuting terrorists or other criminals, and tracing their assets; (b) to financial intelligence units for analysing suspicious or unusual activity, and disseminating it as necessary, and (c) to ordering, intermediary and beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities….*
2. *To accomplish these objectives, countries should have the ability to trace all wire transfers.*

GDF is committed to working with authorities and regulators and we hope you may find this submission helpful.

If you have any questions regarding GDF, the submission, the documents linked to, or in case we can assist you further on this or other topics related to digital finance, please do not hesitate to contact our Executive Director, Teana Baker-Taylor (Teana@gdf.io) or Benedicte Nolens (benedicte@gdf.io) or Malcolm Wright (malcolm.wright@diginex.com) who co-led the drafting of this submission.

Submission

1. Input on 7(b) of the Public Statement as regards to the application of Recommendation 16 ("R16")[4]

7(b) proposes that "*Countries should ensure that **originating VASPs**[5] obtain and hold required and accurate originator information and required beneficiary information on virtual asset[6] transfers, submit the above information to beneficiary VASPs and counterparts (if any), and make it available on request to appropriate authorities.*

It is not necessary for this information to be attached directly to virtual asset transfers.

*Countries should ensure that **beneficiary VASPs** obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers, and make it available on request to appropriate authorities.*

---

[4] Current text for R16:

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain. Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures. Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.
http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

[5] A Virtual Assets Service Provider ("VASP") is defined by FATF as follows:

Virtual asset service provider means 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: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.
http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

[6] Virtual Asset is defined by FATF as:

A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.
http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

Other requirements of R.16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the screening same basis as set out in R.16."

1.1. Virtual Asset Addresses Compared to Traditional Payment Methods

The 7(b) Public Statement presupposes that there is a way for the originating VASP to know who owns the destination address. However, virtual asset addresses differ significantly in the availability of information, as demonstrated below in Figures 1 and 2. They do not contain similar information to existing wire transfer information contained in an International Bank Account Number ("IBAN").

In other words, the originating VASP does not know with any certainty who the destination address is owned by, as there is no register of such addresses and new addresses can be created at any time. By implication, the originating VASP also does not know whether the virtual asset destination address is owned by a VASP, by a non-VASP, or by a natural person.

We illustrate and explain each of these points in more detail below.

Bitcoin address does not contain destination detail

Figure 1: Bitcoin address or "hash"

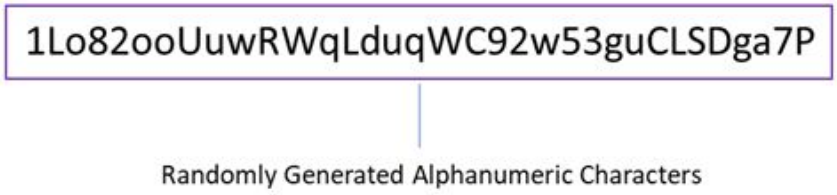
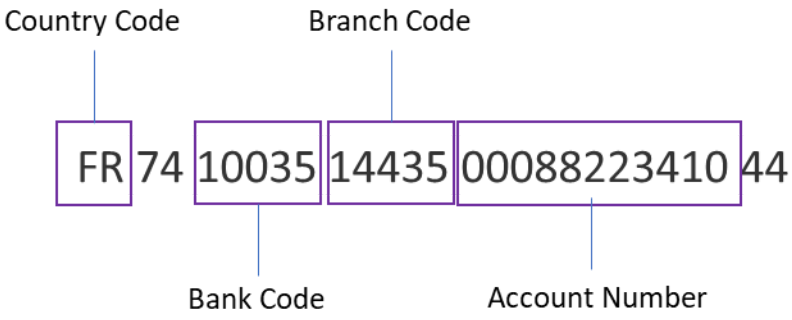


Figure 2 : IBAN number contains destination detail



As can be observed above, an IBAN includes the country, bank, branch, and account number of the transaction originator and beneficiary. Typically, this

would be submitted with a SWIFT BIC code (for the purpose of this illustration, SWIFT is used). This format permits a originating bank to identify and send transaction information to a counterparty or beneficiary bank as the beneficiary bank information is self-contained within the address.

A SWIFT transfer will then typically include all payment instructions included in the Message Type ("MT") messages routed both via originator and beneficiary banks, as well as counterparty banks. Without complete information, the instruction cannot reach the beneficiary bank nor ultimate beneficiary's bank account.

However, a virtual asset address (as demonstrated above with a typical Bitcoin address) lacks all such identifiers. Transmission of value from one virtual asset address to another only requires the address information, and such transactions can take place either through a VASP or peer-to-peer between two counterparties with no VASP intermediaries.

Differences in the virtual asset transaction

In a bank transaction, the transaction value is ultimately sent to a beneficiary bank's private ledger and account. In a virtual asset transaction, the transaction is simply written to the single, distributed ledger for that asset type (e.g. the Bitcoin ledger). Whether a transaction is conducted via a VASP or peer-to-peer, every single transaction is recorded and verified on the same shared ledger which is distributed across a large number of computers.

To write a transaction to the ledger only requires an originator's virtual asset address, a beneficiary's virtual asset address and the value to be moved from one address to another. A date and time stamp are added as the information is written, along with a unique transaction identifier. In the example of Bitcoin, the ledger is public and can be read by anyone.

This means that:

1. An originating VASP (where one is used) does not have knowledge of the beneficiary VASP nor the beneficiary details.

2. The virtual asset holder (i.e. the originator) does not even need to know the beneficiary name nor which VASP they use, if any.

3. The originating VASP simply writes the transaction to the ledger for it to be validated as a legitimate transaction. There is no concept of notification to a beneficiary.

4. The beneficiary VASP (where one is used) *receives* the transaction by reading the ledger and reconciling a change on the ledger in relation to a virtual asset address it maintains. It does not receive any notification

or request from an originating VASP, nor does it know who the originating address belongs to.

5. Even if an originating VASP could collect beneficiary VASP and the ultimate beneficiary's details, there is no way to reliably validate that the details entered are accurate (i.e. if incorrect information is supplied by the originator, it would not prevent the transaction from being written to the ledger).

Creation of new virtual asset addresses is constant and cannot be stopped or prevented

Unlike bank accounts that are created and maintained by a bank, most currently existent virtual asset technologies are public and permissionless[7] which means that there is:

1. No technological way to prevent a virtual asset owner from creating their own payment addresses. Address creation can even be automated and performed at high speed (milliseconds)[8]. Also actors can create an unlimited number of addresses.

2. No technological way to restrict P2P virtual asset transfers between two counterparties.

3. No technological way to understand whether an address belongs to a VASP (which could be a regulated entity where originator and beneficiary information would be required) or a non-custodial wallet (unregulated technology where originator and beneficiary information would not be required).

4. A significant limitation on being able to enforce requirements such as rejecting incoming transfers that lack originator and/or beneficiary information as it is not currently possible to stop incoming transfers.

It is for these same reasons that we believe that it is not possible to capture non-custodial wallets in the regulatory remit of VASPs.

In sum, whereas an IBAN can be easily attributed to a destination bank account with a given bank, the structure of virtual asset addresses means that no such information is available. There is currently no register of virtual asset addresses and even if such a database were available, it would be impossible to mandate that every virtual asset

[7] https://www.coindesk.com/information/what-is-the-difference-between-open-and-permissioned-blockchains

[8] Some wallets (e.g. those that use BIP32 for hierarchical deterministic wallets#) create new addresses automatically in order to protect privacy (e.g. for large players like market makers or exchanges who do not want their positions or trading sizes to be known).

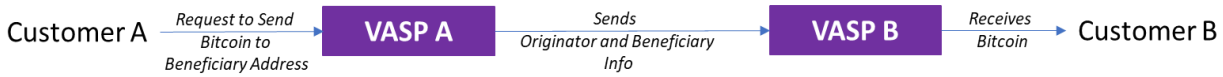
address creator registers their addresses. By implication, such a register would never be complete or reliable.

Even if an originating VASP asked the account holder for beneficiary information before transfer of the assets, the account holder could very easily provide false or misleading information. Furthermore, if he/she does not want to misrepresent but nevertheless does not want to reveal the identity of the destination address, he/she could choose one of the two circumvention techniques below.

1.2. Circumvention of VASP Reporting Requirements

As discussed above, the 7(b) proposal is technically impossible. However, presupposing that it is possible, the intended transaction may then look like Figure 3 below where Customer A uses VASP A to send Bitcoin to Customer B who holds an account with VASP B.

Figure 3

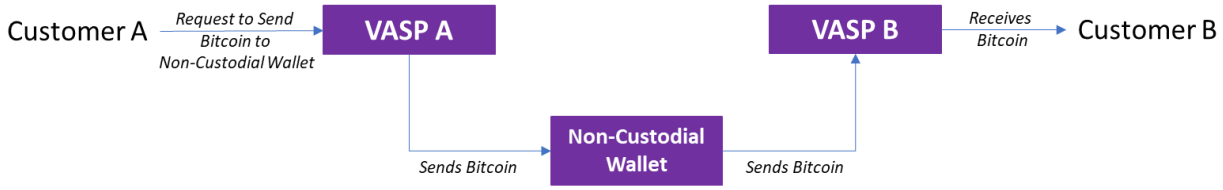


Within this construct, the 7(b) proposal establishes that VASPs A and B must share appropriate Originator and Beneficiary Information. There are two straightforward circumventions to this proposal; both of which are cheap and easy to execute.

Circumvention A: Use of a Non-Custodial Wallet

In Figure 4 below, Customer A requests a transfer to a non-custodial wallet. The holder of the non-custodial wallet may well not be known and the address could easily and quickly be created, as discussed on the previous page. The holder of the non-custodial wallet is then able to submit a transfer onwards to VASP B, which will receive funds without originator information and therefore may assume it is from a non-custodial wallet.

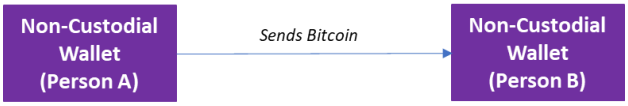
Figure 4



Circumvention B: Peer-to-Peer Transfer

If Customers A and B know each other and hold non-custodial wallets (or can transfer their virtual assets from a VASP into a non-custodial wallet) then the entire transaction can take place peer-to-peer without any VASP interaction, as demonstrated in Figure 5 below.

Figure 5



The ability to easily circumvent a registered VASP would also create challenges around the ability for VASPs to meet the requirements set out under the Interpretative Note to Recommendation 16. These requirements set out the responsibilities of intermediary and beneficiary institutions such as record keeping requirements where beneficiary information is missing as well as the risk-based measures that should be undertaken when information is missing.

The above demonstrates that the requirement set out in 7(b) would be easily circumvented. There is no practical way to stop such circumventions because non-custodial wallets operate on the public internet.

Also, some jurisdictions' constitutions contain provisions (e.g. free speech protections) that might make it difficult to place restrictions on the dissemination and publication of software which might be used to create non-custodial wallets and virtual asset address generation software. Further, many jurisdictions would not place a policy priority on enforcing a ban on such wallets, even if it were to be called for. The outcome of the foregoing, combined with the fact that not all countries are FATF members, would be global regulatory discrepancy and inevitably regulatory arbitrage.

We conclude that the <u>underlined</u> set out in 7(b) on page 3 above is not technically possible and can be easily circumvented and, therefore, would best be removed from the final FATF statement and that, instead, emphasis be placed on the alternative solutions set out under Section 2 below.

1.3. Data Privacy

It is welcomed that 7(b) recognises that data could be stored off-chain as the storing of originator and beneficiary information on a public blockchain may

be incompatible with data privacy legislation such as the EU General Data Protection Regulation if such data were public and immutable.

2. Potential Solutions

Given the technical challenges described under 1.2. above and our recommendation to remove the underlined set out in 7(b) on page 3 above, we now provide alternative solutions to assist FATF in fulfilling the objectives of R16.

2.1. Alternative Solution 1: Robust AML Framework

We support the need for adoption and enforcement of a robust AML framework by VASPs consistent with the FATF recommendations.

Given the lack of availability of wire transfer information, the emphasis on a robust AML framework is paramount; particularly given the VASPs position in providing on/off ramps between fiat currencies and virtual assets.

The current disparity between jurisdictions' approach towards VASPs has resulted in considerable regulatory arbitrage by certain market actors which we believe has been counterproductive to the healthy growth of the digital asset industry.

Therefore, we support the decision by FATF to focus on the application of R10-21 to VASPs, subject to minor comments set out under Section 5 below.

Further, we believe that financial intelligence units (FIUs) can play an important part in enablement of a robust AML Framework. In this regard, we recommend the FATF encourages FIUs to publicise volumes of suspicious transactions reported in the blockchain space, provide information on types of activities reported, and supply the percentage of escalated transactions that belong to recurring wallet addresses or the same client. This will aid VASPs in identifying suspicious activity by establishing common AML criteria and detection logic.

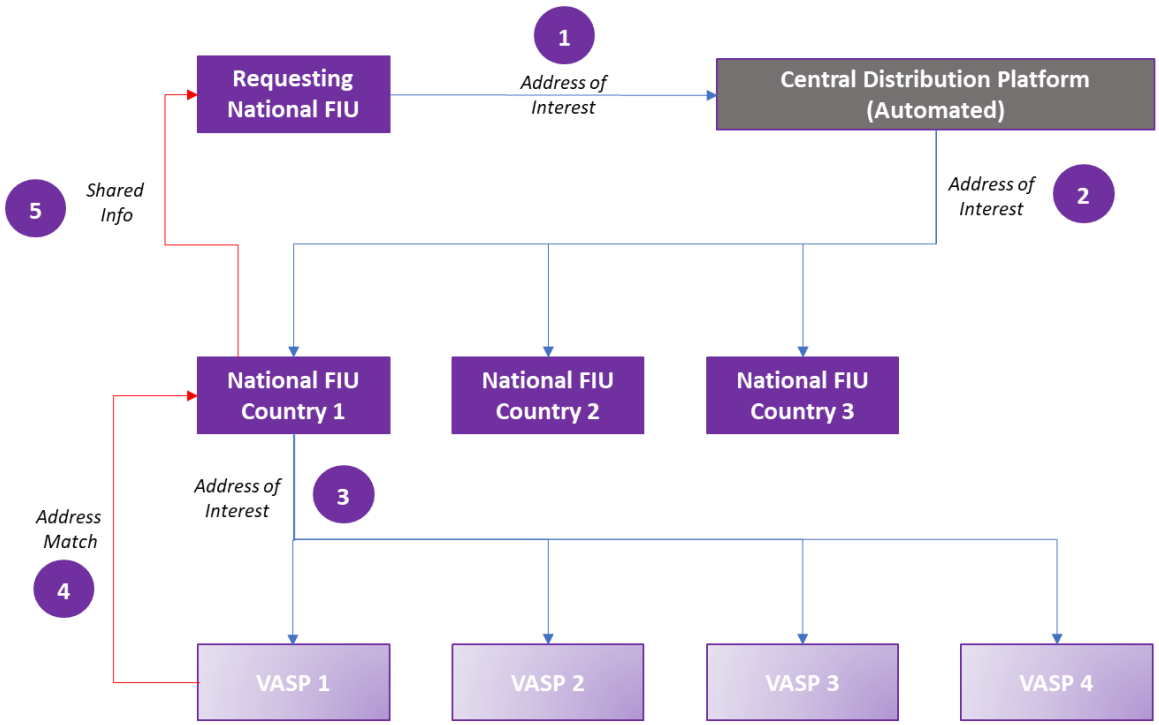
2.2. Alternative Solution 2: Global Public Private Information Sharing Initiative

In a similar way to the United States' PATRIOT Act Section 314(a) framework, FIUs could share virtual asset payment addresses of interest to a global network of national Financial Intelligence Units ("FIUs") who, in turn, would issue requests for information to VASPs in their jurisdiction, who would then report back to their national FIU.

It is considered that such a model would provide for a global response to a global challenge, with minimal technical overhead and supervision, and that would be capable of operating within existing regulatory frameworks, including data privacy. Such a proposal could therefore be implemented within the FATF timeline. Further, it may be possible to automate in a way that could enable rapid responses to FIU requests across borders with minimal time lag, thus enabling a significantly faster response to law enforcement requests and investigations than exists today.

Such a partnership may have challenges that need to be overcome, including governance, technical and legal[9], but would potentially provide the strongest basis for the industry to provide relevant and pertinent information on a push-request basis. Figure 6 and the associated steps illustrates this initiative in practice.

Figure 6



- **STEP 1:** The Requesting FIU Issues an Address of Interest Request (AoI Request) via a central distribution platform. Such information may include the address, currency type, reason code (e.g. Terrorism), and priority (1 – low, 5 – high).

[9] For information on a similar initiative in the traditional finance sector, please see *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime*: https://www.future-fis.com/thought-leadership.html

- **STEP 2:** The platform automatically assesses whether an AoI Request on the same address has been previously requested before issuing addresses to all participating National FIU's. Such a validation step will prevent duplicate requests from being made.

- **STEP 3:** Upon review, the National FIUs issue an AoI Request to all regulated VASPs (and only to such VASPs that would be subject to tipping off legislation). This could be pushed via an automated means so that technology-driven VASPs can minimize manual requirements to check for updates, and potentially respond automatically in a matter of milliseconds.

- **STEP 4:** VASPs that can identify the AoI report back to the FIU accordingly. The information to be reported would be in line with any national legislation.

- **STEP 5:** The National FIU would coordinate with the Requesting FIU to confirm they are able to identify the address. Information would then be shared in line with the National FIU's regulatory framework.

2.3. Alternative Solution 3: Inclusion of Virtual Asset Addresses on Sanctions Lists

The inclusion of virtual asset payment addresses in national-, regional- or international-level sanctions lists, an approach that has already been adopted by OFAC, will assist VASPs in preventing, detecting and freezing transactions involving designated persons/entities.

However, limitations of this approach include:

1. Should a time delay exist between identification of a virtual asset address for designation and the publication of the designated address, the funds may have already moved many times through different addresses from the designated address.

2. Addresses may also be used just one time with funds moving at high velocity between many addresses to hide or obfuscate the flow of value from the originally designated address.

3. Conversely, large numbers of "mischievous" addresses may be used to send multiple small amounts to the designated address to hamper the efforts of law enforcement and VASPs. Such addresses could also be one-time use addresses. As such, any addresses that receive funds from a sanctioned address should not automatically be considered sanctioned themselves. Instead, VASPs should take a risk-based

approach to reviewing those addresses to determine remedial actions to be taken.

4. Once a designated virtual asset address has been published, addresses of a similar nature or owned by the same or related parties may either cease transacting or move their funds to new addresses.

5. Linked to the above, prior to designation, the funds may move to a new address. Designation may need to determine whether downstream virtual asset addresses that have received funds from the designated address should also be sanctioned and if so, how many transaction addresses (or "hops"[10]) away from the designated addresses should be considered as related. However, this in itself creates a dilemma as definition of a specified number of hops could be easily circumvented by a person wishing to move their funds beyond the reach of any sanctions.

2.4. Alternative Solution 4: Centralised KYC Consortia

Consideration may be given to shared KYC utilities whereby such utilities store both KYC and wallet address information that could be made available to law enforcement as well as provide the basis for storing transaction information.

However, it has been observed that to date, implementing even a national KYC utility has been extremely challenging and to do so on an international basis might require significant resources and time to implement effectively and may encounter legal hurdles. Also, it creates data troves that are attractive to hackers. Further, this solution would not solve for the circumvention challenges presented in Section 1.2 above.

2.5 Alternative Solution 5: Decentralized KYC

There is developing technology that enables self sovereign digital identity. This technology allows an individual to store and maintain their identity information, including identity documents, for use by VASPs or other institutions that the individual grants access to. This provides individuals with more control of their information and eliminates centralized data troves.[11]

---

[10] A "hop" refers to the movement of a crypto-asset between one or more intermediary addresses before arriving at its final destination address.

[11] The technology exists in the form of DIDs (decentralized identifiers), verified claims and Identity hubs for globally interoperable, digitally compatible, consumer consent driven information sharing. Identity hubs allow for files to be stored, and accessed via DIDs using customer consent. This enables JavaScript Object Notation ("JSON") readable consumer information, with cryptographically verified identity claims and a full audit trail. DIDs enable a requesting party to receive a JSON object with customer information, alongside national documents and verified claims. This information is shared securely, and can be mathematically verified. This solution is decentralized and

The adoption of this technology is still in early phases, but once adoption increases, it can be helpful at meeting the goals of R16.

3. Benefits of blockchain for law enforcement and information sharing

While the underlined in 7(b) is not achievable, blockchains that underpin virtual asset address transactions have some unique advantages that, if seen as part of the broader evolution of technology, are already being used by law enforcement to track down crime.

Such blockchains are public, shared databases that record virtual asset transactions between two counterparties. After a particular transaction is validated and cryptographically verified by validating computers on the blockchain's network, it is then made into a "block" on the blockchain. Once recorded as a block, transactions are ordered chronologically, timestamped, and cannot be altered or changed.

Though the information contained in virtual asset transactions varies depending on the virtual asset that is being used as a means of transfer, many popular virtual assets include the following basic information:

1. a unique transaction ID to identify the transaction;
2. the date and time of the transaction;
3. the value of virtual assets being transferred; and
4. the source and destination virtual asset addresses of the transfer.

This level of transparency can be useful where this transactional information can be attributed to specific criminal actors, such as terrorists, illicit online vendors, or cybercriminals. It may then be possible to obtain a degree of insight about those actors' financial activities that is often not possible to obtain in the traditional, fiat sector.

Blockchain forensic and bespoke AML compliance software tools, together with open source intelligence (OSINT), exist that enable VASPs to engage in the monitoring of such activity, and law enforcement agencies have utilized these tools as well to successfully detect and prosecute criminal activity, as evidenced by several high-profile cases. Due to the linked nature of transactions, the use of such tools allows for funds to be instantly traced back through the history of prior transactions of the same virtual asset; something that is not possible in the traditional financial sector without significant

provides for an open platform upon which any company can build without vendor lock-in. Such a system is self sovereign - allowing the user full control and consent mechanisms, in line with national data regulations requiring consent. Certain companies and foundations that are actively working on these types of solutions (DIF, KYC-Chain, SelfKey, Civic, Uport, Sovrin, Microsoft, w3c and many others). More information at identity.foundation .

overhead and data privacy challenges. Patterns of activity can also be easily established, where funds have attempted to be layered.

Such tools proved especially vital in cases involving dark web marketplaces, and in instances of ransomware attacks and other cybercrime activity. For example, blockchain forensic software tools have been publicly acknowledged as having played a role in the law enforcement actions involving the Alphabay dark market, as well as in cases of online arms dealing and other crimes[12].

Whilst such tools have clear benefits to the industry and law enforcement, it should be noted that they are not effective in the case of virtual assets with privacy-preserving features (such as Monero). Such virtual assets may see continued adoption, including for legitimate reasons of desiring transaction privacy or seeking protection from being monitored by cybercriminals. Therefore, it is important that FATF not solely place reliance on the efficacy of blockchain forensic software tools, but also consider the proposed solution set out under Section 2.2. above.

Finally, certain virtual assets have a "freezing" capability built into them, which can be highly beneficial for law enforcement. There are examples of this being put into action already in the case of stable coins backed by fiat. For example, in the case of the stable coin USDC[13], the stable coin issuer reserves the right to "blacklist" certain addresses and freeze any virtual asset address that the issuer suspects is associated with illegal activity. The issuer also reserves the right to terminate the account and report such suspected illegal activity to applicable law enforcement agencies, who in turn may require the assets that are frozen be surrendered.

4. Other input on the Public Statement

4.1. Input on 1 of the Public Statement

According to 1, *"For the purposes of applying the FATF Recommendations, countries should consider virtual assets as "property," "proceeds," "funds", "funds or other assets," or other "corresponding value". Countries should apply the relevant measures under the FATF Recommendations to virtual assets and virtual asset service providers (VASPs)."*

The FATF definition of virtual asset[14] is focused on tokens that can be used for *"payment and investment purposes"* and that are not already captured by

[12] https://www.wired.com/story/hansa-dutch-police-sting-operation/ and https://www.technologyreview.com/s/610807/sitting-with-the-cyber-sleuths-who-track-cryptocurrency-criminals/

[13] https://www.circle.com/en/usdc

[14] FN 5: "A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations."

regulation. However, the language underlined above casts the net much more broadly, and possibly too broadly.

In particular, as explained in the GDF Taxonomy[15] tokens serve different purposes. The GDF Taxonomy distinguishes between *Consumer Tokens*, *Payment Tokens and Financial Asset Tokens*. Not all these tokens can, or should, be categorized as underlined above under existing national laws.

Consumer Tokens (similar to so-called "utility tokens") should not be captured in AML regimes, especially when the tokens are being used for intended consumptive purpose - e.g. Ether paying for computation on the Ethereum blockchain, or a token being used like a movie ticket to attend a show, or a tokenized loyalty program such as airline miles[16].

These applications are currently not captured in AML regimes. Converting the tracking and awarding of such programs to blockchain should not trigger them to be included in such regimes. Doing the opposite would constitute material overreach. It would also be very complex to enforce, even more so considering the number and variety of Consumer Tokens that may be developed in the future[17].

---

[15] https://www.gdf.io/resources/

[16] The GDF community selected the term "consumer token" instead of "utility token" because it properly emphasises that for a Consumer Token to become successful, it needs adoption by actual consumers who will use and consume the token. We recognise that this implies the need for potential consumer protections. Whilst many of these tokens are still early as are the platforms that support them, the GDF community aims to strike the right balance of enabling innovation whilst being committed to efficient, fair and transparent market activity (where reasonably applicable). Per P7-8 of the GDF Taxonomy, consumer tokens can represent: (i) Consumer Ownership Rights: Tokens can themselves be a natively digital consumer good, such as a tokenised collectible like a badge for online gameplay or a unique digital collectible that does not exist in the physical world, such as a virtual pet; or they can represent ownership of an analog (i.e. not digital or on the blockchain) good, such as a traditional baseball card. In these cases, the token can confer ownership in the corresponding good and/or represent the good. (ii) Consumer Coupon Rights: Tokens that provide a partial or complete discount on particular goods, services, or content, in the physical world or in the virtual world, e.g. file storage on a given token-powered network or electricity provided to retail customers. (iii) Consumer Activity Rights: Tokens that involve rights or obligations related to an individual user's activities on a token-powered network. With regard to consumer activity rights, we contemplate at least two current subcategories: (a) Reward: Tokens that serve as a form of reward or payment for performed activities. In the cases of online platforms, the tokens earned can also be used to access features or get benefits on the platform. In the case of physical systems, the tokens may act like "frequent flyer miles" to be redeemed for services or goods. (b) License: Tokens that serve as a means to access or perform certain activities related to a blockchain or online service. Analogies in the analog world may include a software license, taxi medallions for New York City taxis, or occupational licensing and certifications for certain vocations. In the virtual world, this could include a token which allows access to a content-driven website. License rights may also include relationships similar to those we are all familiar with, such as a membership to a wholesale club, or the right to participate in a book club of the month. The term "utility token" has also been used to describe what this document calls "consumer tokens."

[17] For example, while the details are not yet known, Emaar Group, one of the United Arab Emirates' largest real estate developers and the firm behind the Burj Khalifa, announced that it is planning to develop the "Emaar community token" for its customers and partners by the end of 2019.

Furthermore, classifying tokens through the use of generic terms such as the language underlined above risks inadvertently triggering implications under other standing national laws, for example tax laws. They risk not being compatible with standing national laws[18].

Therefore, we consider that rather than provide a wide suggestion as above, reference be made to existent Token Taxonomies and a decision be made that Consumer Tokens should not be captured in the national implementation of the FATF recommendations.

One way would be to explicitly exclude Consumer Tokens (including Utlity Tokens) from the FATF definition of a virtual asset. Another way is to clarify the same in the Public Statement.

4.2. Input on 2 of the Public Statement

According to 2, *"In accordance with Recommendation 1, countries should identify, assess, and understand the money laundering and terrorist financing risks emerging from virtual asset activities and the activities or operations of VASPs. Based on that assessment, countries should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. Countries should require VASPs to identify, assess, and take effective action to mitigate their money laundering and terrorist financing risks."*

In 2018 Europol highlighted that approximately EUR3-4 billion of criminal money is being laundered through crypto assets linked to[19]:

1. Their use to support black market transactions on the dark web.
2. Theft through fraudulent ICOs.
3. Hacks on echanges which as at the end of 2018 totalled $1.5billion, with $865m stolen from 6 hacks in 2018[20].
4. Sanctions evasions by state actors.

Given that it is estimated that between $800billion to $2trillion is being laundered through the global financial system annually[21], it is clear that the risks in the current virtual asset system are currently very small/less than 1% when compared to those in the traditional financial system.

---

[18] For example, it may be inconsistent with the UK approach proposed in the published reports: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf ; https://www.fca.org.uk/publication/consultation/cp19-03.pdf .

[19] https://www.bbc.co.uk/news/technology-43025787

[20] https://www.coindesk.com/2018-a-record-breaking-year-for-crypto-exchange-hacks

[21] https://www.unodc.org/unodc/en/money-laundering/globalization.html

Also, while there has been a growing trend in the use of virtual assets to launder funds as criminals become more confident in using new technology, there is a big correlation between this upward trend and the wider adoption of virtual assets for legitimate purposes particularly given the growth of the number of blockchain protocols and use cases (e.g. parties wanting to invest in blockchain protocols or using tokens for use or consumption - we refer in this regard to the GDF taxonomy).

In view of the above, it is sensible for FATF's response and that of the member countries to be commensurate to those more limited risks at this time.

4.3. Input on Section 3 of the Public Statement

According to Section 3, *"VASPs should be required to be licensed or registered. At a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created. In cases where the VASP is a natural person, they should be required to be licensed or registered in the jurisdiction where their place of business is located. Jurisdictions may also require VASPs that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a VASP. Countries should take action to identify natural or legal persons that carry out VASP activities without the requisite license or registration, and apply appropriate sanctions."*

In respect to the underlined, while licensing or registration for AML compliance purposes would be reasonable, the FATF should seek to provide guidance with regards to proportionality as well as promoting harmonisation across jurisdictions.

The unintended consequences of a lack of proportionality and harmonisation may lead to overburdening VASPs and consequently removing one of the most effective forms of prevention and partnership law enforcement currently benefits from in the virtual asset sector.

4.4. Input on 7(a) of the Public Statement

According to 7(a), *"The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000."*

The working group noted this threshold is low, especially when taking into consideration that the median Bitcoin transaction appears to be around 250

USD[22]. Also, given the price volatility of crypto assets, a low threshold may be hard to implement as transactions may at a given time be below, and soon after above, the USD/ EUR 1000 threshold. For example, in a down market, occasional microtransactions or mining conducting through a VASP may never meet a *de minimis* threshold, but if the market swings dramatically, then all of the transactions or values may surpass the threshold. There is a risk at this point that the VASP, that would normally be outside the scope of these requirements, suddenly finds itself subject to requirements that it may not have the infrastructure to support.

Furthermore, it is recommended that FATF clearly indicates when the *de minimis* threshold should be calculated. With a *de minimis* threshold currently set in fiat, this will inherently require a conversion calculation to determine the fiat value of the cryptocurrency at a specified time. Given that the threshold is being calculated for the purposes of conducting due diligence, completing it after the transaction occurrence will lead to difficulty in enforcing the collection of due diligence information. Completing at the point of transaction request may lead to a delay in transaction execution, and give rise to complaints from customers with regards to unfair treatment, loss of profits, etc.

As such, it is recommended that FATF update the Interpretative Notes to reflect that this calculation should be made at the point in time in which the transaction occurs, and note the consequential impact that VASPs and countries should seek to mitigate.

5. Comments on Recommendations 10-21

VASPs operating in jurisdictions that have made statements about future policy direction[23], or that have already issued guidelines or legislation bringing such VASPs in the remit of AML regulation, are more likely to have started implementing normal course AML/CFT measures, including:

1. Risk assessments (R1)
2. Sanctions screening for customers and payments and reporting of sanctions breaches (R6 and R7)
3. Customer Due Diligence (R10)
    - KYC
    - EDD

[22] https://bitinfocharts.com/comparison/mediantransactionvalue-btc.html#6m

[23] Some recent clarifications include importantly the FATF statement of October 2018 as well as those from the UK FCA (Nov 2018), the HK SFC (Nov 2018), the EBA (Jan 2019), the Singapore MAS (Jan 2019), etc.

    - Surveillance and transaction monitoring - both fiat/crypto and crypto/crypto

4. Record-Keeping (R11)
5. PEP name screening (R12)
6. Reliance on third parties, particularly with regards to CDD (R17)
7. AML staff training (R18)
8. SAR/STR reporting to local FIUs and law enforcement (R20)

FATF's position set out in 7(a) that "*with respect to preventive measures, the requirements set out in Recommendations 10 to 21 apply to VASPs*"[24] will further accelerate this evolution.

GDF undertook a line by line read-through of the FATF 40 Recommendations and identified 3 recommendations that require further clarification in R10-21, noted as follows.

5.1 Recommendation 10: Customer Due Diligence

It is requested that the FATF clarify:

- Whether the opening of an account, wallet or other similar facility by a VASP for a customer amounts to the establishment of a business relationship to trigger CDD requirements in and of itself in the absence of any transactions (both deposits and withdrawals).
- Under what circumstances VASPs may be considered to represent lower risks for AML/CFT purposes.
- The definition of a "transaction" in the context of virtual assets.
- That blockchain-specific forensic analytics tools, bespoke AML compliance software, and other due diligence and monitoring measures may be applied to implement the risk-based approach to manage risks in the case of virtual assets, in line with comments and caveats discussed earlier in this letter.

5.2 Recommendation 11: Record-Keeping

It is requested that the FATF clarify:

- That the immutability of blockchains can be relied upon for record keeping. In other words, a VASP does not need to keep a full copy of an

[24] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html

entire public blockchain ledger in order to fulfil record-keeping requirements.

5.3 Recommendation 17: Reliance on 3rd Parties

It is requested that the FATF clarify:

- Whether a VASP might be considered as a "Financial Institution" for the purposes of enabling other VASPs and FIs to rely on a licensed VASP's CDD/KYC (identification and verification and record keeping of their customer). This would streamline customer onboarding and help build up the global KYC sharing consortium identified in 2.4 above.

5.4 Recommendations 22 and 23: DNFBPs

Although Recommendations 22 and 23 were not referenced in the FATF February 2019 statement, it is requested that the FATF:

- Make reference to VASPs for alignment purposes with the October 2018 statement[25] should VASPs be considered as Designated Non-Financial Businesses and Professionals ("DNFBPs"). This may include guidance towards the activities which may be considered DNFBP activities as opposed to those more aligned to FIs.

- Consider adding reference to virtual assets in addition to the use of "cash transaction" in Recommendations 22(c) and 23(b) which includes measures for dealers in precious metals where, for example, the same transaction could take place using a virtual asset instead of cash. This is not to classify VASPS in these Recommendations rather to ensure that a loophole is closed whereby virtual assets might be used as a payment method in place of a "cash transaction".

[25] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html

Supporters of this Letter

- Musheer Ahmed, Managing Director, Fintech Association of Hong Kong
- Simon Au-Yeung, COO, HashKey Group
- Daniele Azzaro, CAMS, AML Specialist, Individual Contributor
- Teana Baker-Taylor, Executive Director, GDF
- Jeff Bandman, Board Member and Advisory Council Member, GDF, Principal, Bandman Advisors
- Martin Baumann, Managing Partner, CMCC Global
- Brian Brooks, Chief Legal Officer, Coinbase
- David Carlisle, Head of Community, Elliptic
- Boon-Hiong Chan, Individual Contributor
- Xenia Chen, CAMS, AML Specialist, Individual Contributor
- Gus Coldebella, Chief Legal Officer, Circle
- Araba Eshun, CCO, Coinfloor
- David Fauchier, CIO, Cambrial Capital; Advisory Council Member, GDF
- Olga Feldmeier CEO, SMART VALOR
- Tyler Frederick, CFA, Compliance Manager, Circle
- Jack Gavigan, Individual Contributor
- Ellis Gyöngyös, CEO, Know Your Token
- Charles Hayter CEO, CryptoCompare, Advisory Council Member, GDF
- Thomas Hook, AML Compliance Director, Circle
- Mark Kelly, Head of Compliance UK, Coinbase (CB Payments Ltd)
- Samson Leo, Chief Legal Officer, XFERS
- Juan Llanos, Individual Contributor
- Edmund Lowell, CEO, KYC-Chain Ltd.
- Neeta Patel, Chief Compliance Officer, R3
- Matthew Pollard, CFO, Archax, Advisory Council Member, GDF
- Hugh Madden, Executive Director, CTO, Branding China Group, CEO, Co-founder and CTO, ANX International
- Urszula McCormack, Partner, King & Wood Mallesons
- Ben Morley, CEO, Digax
- David Nicol, Head of Digital Assets, R3, Advisory Council Member, GDF
- Benedicte Nolens, Chair Advisory Council, GDF, Head Regulatory Affairs Asia and Europe, Circle
- Neepa Patel, Chief Compliance Officer, R3
- Denisse Rudich, AML/CFT Working Group Co-Lead, GDF, Director, Rudich Advisory
- Ryan Selkis, CEO, Messari, Advisory Council Member, GDF
- Alexandra Sowa, General Counsel, SMART VALOR
- Elaine Sun, Compliance Director, Huobi Group
- Leonie Tear, Senior Associate, King & Wood Mallesons
- Lawrence Wintermeyer, Co-Chair and Advisory Council Member, GDF
- Malcolm Wright, AML/CFT Working Group Lead, GDF, Chief Compliance Officer, Diginex