

Vice President Dombrovskis
European Commission

Wednesday, 17th June 2020

Dear Vice President Dombrovskis,

I hope you, your family and the staff at the European Commission are keeping safe and well during this challenging time.

We are writing to you regarding the so called “Travel Rule” consisting of [the new FATF Recommendation 16](#) (R.16). In principle, we are supporting the establishment of rules allowing for a more effective fight against money laundering and the financing of terrorism (AML / CFT) and more generally against fraud and tax evasion. As such, we share the FATF R.16 objective of implementing a unified and comprehensive regulation applicable within all FATF member states and to all Virtual Assets Services Providers (VASPs) players in scope of the recommendation.

At the same time, we would like to draw your attention to aspects of R.16 which pose serious questions in terms of both the consistency of the proposed measures and of the risks such measures would entail. We also highlight other aspects of R.16 which make them unenforceable in practice, contrary to European law and potentially harmful to European competitiveness and sovereignty. Moreover, we also would like to observe that by implementing *mutadis mutandis* some rules that exist in the financial world (like the travel rule as detailed below), one has forbidden the specific nature of the blockchain ecosystem and the fact that each and every transaction is traceable¹. VASPs’ ability to help enforcement bodies tracking criminals has already shown that where crypto-currencies are involved criminals have little chances to escape, unless of course they are able to come back to fiat/cash which, not being traceable, represents a higher risk.

In February 2019, the FATF set out detailed implementation requirements for regulation and supervision and monitoring of VASPs. FATF has therefore been working on R.16, amending Recommendation 15 in October 2018 to clarify how the FATF standards apply to activities or operations involving virtual assets. The text of R.16 was adopted as part of the [FATF Standards](#) in June 2019. The FATF will monitor the implementation of the new requirements by countries and service providers and conduct a 12-month review in June 2020, which is this month. We are consequently writing to you to bring your attention to this matter and ask for your support to implement realistic measures.

R.16 requires that countries should ensure that VASPs from which a transfer is made: (i) include accurate originator information as well as (ii) information on the beneficiary of virtual asset transfers and (iii) submit those data to the VASP that hosts the beneficiary of the transfer or financial institution (if any) immediately and securely, and make it available on request to the

¹ Except for the so-called « *privacy coins* »

relevant authorities.

The contemplated system is *mutatis mutandis*, mirroring the existing regulation applicable to financial institutions.

Countries should ensure that beneficiary VASPs obtain and hold the required originator information and the required and accurate beneficiary information on virtual asset transfers, and make it available on request to the appropriate authorities. The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.

Furthermore, R.16 Chapter c regarding cross-border qualifying wire transfers sets out the required information which shall accompany all qualifying wire transfers:

- (a) the name of the originator;
- (b) the originator account number where such an account is used to process the transaction;
- (c) the originator's address, or national identity number, or customer identification number, or date and place of birth;
- (d) the name of the beneficiary; and
- (e) the beneficiary account number where such an account is used to process the transaction.

In June 2019 the BVC WG submitted its comments about R.16 to the FATF Secretariat and to FATF Member States. The BVC WG comments included the following three key points:

1. There are data protection and GDPR-compliance concerns due to a potentially unlimited data export of personal data from EU citizens and companies to all countries in the world;
2. There are practical limitations to accurately verifying the identity of the beneficiary (e.g. when the address is not controlled by a VASP); and
3. The recommendation could lead to a 'cobra effect', as users who care about privacy could be driven to conduct virtual asset transfers without using VASPs and migrate to decentralised exchanges, reducing traceability and weakening AML controls.

These concerns were already voiced by the BVC WG during the Plenary of the Financial Action Task Force, the 2019 FATF PRIVATE SECTOR CONSULTATIVE FORUM (FATF PSCF) which took place in Vienna, Austria, on the 5th and 6th of May 2019. Despite strong acknowledgment of such concerns by many of the Consultative Forum attendees during the forum, such remarks have been largely ignored by FATF.

We are therefore now reaching out to you as the above-listed facts create a problematic situation for European companies active in this sector, a situation which could hinder the possibility to have fair competition conditions between European and non-European based entities in this sector.

1. There are data protection and ECHR/GDPR-compliance concerns due to a potentially unlimited data export of personal data from EU citizens and companies to all countries in the world:

As outlined by the European Commission in the recently published [Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing](#), "The obliged entities, when accessing information relevant for carrying out customer due diligence, and public authorities exchanging information between them, including outside the EU, must fully comply with the EU data protection legislation. For example, providing obliged entities with access to certain publicly owned registers might raise data protection concerns. The difficulty to ensure compliance with data protection and confidentiality was also mentioned in the context of exchange of information between competent authorities. These issues should be duly addressed".

We would like to note that a tension between the regulatory objectives of protecting human rights as enshrined in the European Convention of Human Rights (ECHR) and the need to combat criminality has also been explicitly identified by the Dutch Data Protection authority.² The main consideration is in this case whether the regulatory measures in the area of prevention of money laundering are sufficiently specific and proportionate when tested against the right to privacy and the presumption of innocence in the ECHR. In this respect the Dutch Data Protection has advised the Dutch Ministry of Finance that the envisaged evaluation under article 65 of the fifth Anti-Money Laundering Directive (AMLD5) is used for this fundamental debate.

Complying with R.16 would require channelling the data relating to transfers through a global organisation, such as – for example - the G20, to cluster all the information about the addresses in one central data point. This, however, may conflict with the GDPR, as the central data point would be vulnerable to hacks. Moreover, questions are raised about the location in which this data would be kept, if for example this data had to be hosted in the US – by a private or public US entity - this could allow US authorities to access EU citizens' personal data, which again could conflict with the GDPR.

In this respect we would like to point out that it was suggested to the FATF, during their public consultation process, to apply a domestic regime for the travel rule to jurisdictions such as the EU in order to allow for a domestic regime of “request based” provision of personal data, when the need arises. This has however been explicitly discarded in consideration 113 of the FATF guidance. We would therefore urge the Commission to consider such a domestic regime within the EU. We would find it hard to envisage a future where the EU, seeking to promote the innovation in the area of blockchain and distributed ledger technology, at the same time promotes disproportional personal data export.³

While we draft this letter to you, we have yet to see whether a workable industry-wide solution for implementation would be available. The issue is that the originator and beneficiary information cannot travel with the virtual asset transaction itself. In other words, this personal information cannot be stored on the public permissionless bitcoin network. The industry therefore needs a separate layer for communication between the VASPs to exchange this information. This communication system would need to be up and running by June 2020 – now - and all VASPs globally would need to have access to it.

We have not seen any operational global solution in the market for the time being, and there is certainly no European-based solution that is operational and available at the moment⁴. Currently there is no secure channel for VASPs to communicate these data; while most VASPs already

² Legislative advice by Autoriteit Persoonsgegevens, dated Mart 7, 2019, available at: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_wijziging_vierde_antiwitwasrichtlijn.pdf and dissertation of C. Kaiser: Privacy and Identity Issues in Financial Transactions, Groningen, 2018, available at: https://www.rug.nl/research/portal/files/65647303/Complete_thesis.pdf

³ We also point out that in the 20 years of its existence the Travel Rule has not been properly evaluated and has not been demonstrated to be effective. See the dissertation of M. Wesseling; The European fight against terrorism financing: Professional fields and new governing practices, Amsterdam, 2013, available at https://pure.uva.nl/ws/files/1737805/126131_thesis.pdf.

⁴ Some initiatives have already started but none came to the conclusion that a viable solution could be ready by the end of June, far from it. InterVasp organization (<https://intervasp.org/>) has released a data format protocol which has to be implemented on technical solutions. As for the technical solutions themselves, we have been made aware of the OpenVasp Swiss initiative (<https://www.openvasp.org/>) and Ciphertrace initiative (<https://ciphertrace.com/trisa-unveiled/>) but none of them is currently up and running.

successfully and securely store information on their customers, it is the requirement to securely submit this information to other VASPs that is proving most challenging. It therefore seems unlikely to the BVC WG that there will be a workable solution to fully comply with the Travel Rule by the end of this month. Therefore, what the BVC WG is looking for is a way to discuss with European and national regulators in Europe about what VASPs can actually do and what would be helpful to make the industry safer in terms of AML risks.

In addition, the need to simultaneously transmit the information (surname, first name, date of birth / nationality, etc.) of the initiator (natural or legal person) to a VASP that is located anywhere in the world raises questions about feasibility, the format to be used, security and compliance with the GDPR or equivalent rules (use of data, storage location, possible hack) and more generally on the confidentiality necessary for certain transactions.

For example, there are cases where European state structures or European state institutions carry out transactions; these data are sensitive and the implementation of R.16 in these cases cannot be carried out lightly and without international consultation, while at the same time taking into account European states and companies interests. These institutions may send cryptocurrencies to an address held by one of their customers, such as an individual or another institution. It will be very complex for the industry to ask its institutional customers to declare the name of their own customers. The institutions in question will be extremely reluctant to do this, because of competition concerns or due to privacy agreements they may have in place with their customers. These are European institutions that are regulated and carry out KYC, AML checks etc, but they may be uneasy to share information with a VASP, as is understandable.

The United States has proposed a “home” solution in Vienna based on x509 (PKI). Besides the fact that the proposed solution is a commercial attempt with a technology controlled by a US company, it is especially completely irrelevant. When dealing with such technological challenges and international competition, it is crucial to consult scientists and experts in Blockchain and Data technology. It is of crucial importance that the solution provided be global, open source and free. If not, the crypto ecosystem will be made of “large” VASPs that can afford such compliance and will lead the smaller actors with no other exit than closing their doors.

Moreover, what the BVC WG would like to avoid is seeing EU citizens’ personal data being submitted to third countries which do not have the same data protection standards, such as the U.S. Another issue we foresee is that if the infrastructure necessary to comply with R.16 is a non-European infrastructure, it would mean that Europe will depend on factors that are outside of its jurisdiction. This has been pointed out in the past by the **Commission President, Ursula von der Leyen**, who stated that EU citizens must have access to a common digital market. This would be increasingly difficult if important structural digital tools and solutions are designed outside of the EU. In other words, recent developments could lead to third country industry giants growing while no European company would be able to grow, unless the European Commission takes the initiative rather than let the FATF and some countries lead the way.

Furthermore, R.16 may have worrying political implications, as for example this may result in “a local law enforcer in an undemocratic country getting EU data by harvesting its home companies data for the EU-info, without having an appropriate legal warrant under EU-rules” as explained in very clear terms by Simon Lelieveldt, payments and blockchain expert, ex Senior Policy Analyst Retail Payments and E-money at the Dutch Central Bank (DNB) and ex Head of Department on Banking Supervision and Financial Markets for the Dutch Bankers Association ⁵.

2. There are practical limitations to accurately verifying the identity of the beneficiary (e.g. when the address is not controlled by a VASP):

We would like to highlight the lack of technological solutions to comply with this aspect of R.16, and the consequent difficult and easily circumventable implementation of R.16.

To date, there are no systems capable of determining precisely and in each case, who owns a cryptographic wallet address. It is possible to generate on the fly, if desired, an infinite amount of addresses. Building a global map, up to date at all times and searchable in real time of the Blockchain is unrealistic and denies the very specific nature of the blockchain system.

Much of the implementation of R16 will therefore be based on the declaration of the person responsible for the transfer. If this person declares that the beneficiary is their account with another VASP, it will be possible to verify this by using chain analytical tools and interfacing with this VASP to transfer the information. However, the initiator may declare that he or another person is the beneficiary. The verification of this information from a provided address is not guaranteed. While no mapping is possible, the initiator can lie on the name of the beneficiary and the blockchain analysis tools can only provide partial responses and no interconnection at all times with all VASPs around the world.

In fact, VASPs are distributed all over the world and for many in non-European jurisdictions, often singled out for their lack of rigor in AML / CTF matters where regulation is weak. It is therefore difficult to set up data exchanges on both sides with actors who refuse to do so. The R.16, would not work in this scenario and would allow that malicious people or organizations easily get around the difficulty despite the R16. We are therefore in the opinion that the implementation of R16 would, in the end, be detrimental to the prevention of money laundering.

While the BVC WG recognises FATF’s critical role in the fight against money laundering and terrorism financing and BVC WG and its members are committed to the prevention of money laundering and terrorist financing, we would like to note that, - as the European Commission has proved thus far while drafting the 5th AntiMoney Laundering Directive- in rulemaking for virtual assets it is important to be aware of the characteristics of virtual assets and their supporting technologies (such as blockchains). Moreover, in this specific case, it is important to understand the differences in the nature of virtual asset transfers and bank wire transfers. For example, virtual asset transfers performed according to a blockchain protocol are completed without any involvement of intermediary financial institutions. Therefore, despite the effortlessness of cross-border transfers of virtual assets, VASPs will not always be able to identify or manage originators or beneficiaries, while this is possible for bank wire transfers.

The BVC WG understands that most companies that would fall under the definition of a VASP in R.16 already comply with these requirements, as far as they identify their customers and as such can also identify the sender of a virtual asset transfer that has been performed via their wallets on behalf

⁵ https://www.linkedin.com/pulse/fatf-eu-need-fundamentally-rethink-approach-virtual-simon-lelieveldt?articleId=6532243583704014848#comments-6532243583704014848&trk=public_profile_post

of a customer. However, most members of the industry have so far abstained from also identifying the recipient of a virtual asset transfer. The most important reason for this is that in many cases only the sender of the virtual asset transfer can provide the name of the beneficiary and there is often no possibility to verify the information on the identity of the beneficiary provided by the sender.

The application of R.16, would have in the BVC WG view, several implications in this respect:

- Companies from the virtual asset sector would need to ask the sender of a virtual asset transfer to provide information on the identity of the recipient of the transaction.
- Whenever a virtual asset transfer is performed on behalf of a customer the company would need to be able to establish if the target address is being controlled by a VASP.
- Therefore the sender would either also have to provide the name of the VASP controlling the target address or there would need to be some kind of a register that attributes all existing custodial wallet crypto addresses to their corresponding VASP.
- Furthermore this information would need to be transmitted to the VASP controlling the target address.

Many members of the industry attended the FATF PSCF in order to receive clarification on this controversial recommendation and its implications. Several questions on how exactly the recommendation could be implemented have been brought forward:

- How exactly would a VASP determine if a certain crypto address is being controlled by another VASP?
- How can a VASP verify the information on the identity of the beneficiary of a virtual asset transfer, especially if the target address is not controlled by a VASP?
- How exactly should the exchange of information between the VASP of the sender and the VASP of the beneficiary take place?

These questions have not been answered by the FATF as of today.

Notably a VASP typically provides its customers with more than just one single crypto address and the wallets of larger VASPs can easily consist of several million crypto addresses.

At this stage, we would like to emphasize that the US, which have been assessed as largely compliant by FATF no later than in March 2020, have implemented the travel rule not asking for checks of the recipient address and not making the collection of the recipient address compulsory⁶.

The travel rule has not been amended for crypto purposes in the US and FATF has not commented on this thus far. In our view, any stricter implementation in the EU would make the EU losing a significant competitive advantage.

As it's not always easy to identify who the beneficiary is in the virtual assets context, the BVC WG believes all that should be required under the FATF Guidance is that the VASPs try and identify the beneficiary "**to their best efforts**". Two good ways of establishing beneficiary information could in our view be: 1. the use of search engines specialised in linking specific wallets to their owners OR 2. directly asking the client and not impose on the VASPs any accuracy checks (as is done in the US). As we can never achieve perfect accuracy, a VASP could be deemed in the BVC WG view to

⁶ extract from <https://www.sec.gov/about/offices/ocie/aml2007/fincen-advisu7.pdf>

have done everything they can to mitigate risk if they've asked their client for the beneficiary information. If the VASP takes a consistent risk-based approach, then it shall in our view be compliant. More precisely, R.16 explains that only the originator information must be '*accurate*', while beneficiary information is only '*required*'. This is likely to be because you cannot reject a transaction in a vcs context, whether the information on the beneficiary is accurate or not. This further suggests that VASPs implementing the requirement '*to their best efforts*' would be sufficient.

Even if the "best efforts approach" above was retained as the European approach to R.16, the main issue would still be that R.16 would ask the originator VASP to '*immediately and securely*' send the information to the beneficiary VASP. The BVC WG would like to note in this respect that there is currently no way to transmit this information in such a way.

3. The Recommendation could lead to a 'cobra effect' as users who care about privacy could be driven to conduct virtual asset transfers without using VASPs and migrate to decentralised exchanges, reducing traceability and weakening AML controls:

Furthermore, some companies have voiced the concern that the implementation of the FATF recommendations could lead to a [cobra effect](#) meaning that it could have the opposite effect of what was intended to be achieved in the first place: more efficient measures to combat money laundering and terrorism financing in the virtual asset sector. Users who care about privacy and do not want to be thoroughly examined could be driven to conduct virtual asset transfers without using VASPs and might migrate to decentralized exchanges, therefore reducing the traceability of virtual asset transfers as a whole and strengthening the ecosystem of decentralized exchanges that is still in an early stage.

**

In consideration of all the above, and given the global nature of virtual currencies and the fact that additional deposit addresses are easily created, the BVC WG believes that complying with the requirements of R.16 would be ineffective.

Moreover, we see an issue in terms of competitiveness for European companies. And we consequently believe that an involvement from the European Commission would be highly desirable, despite the fact that it is not the European Commission but the Member States which will be audited by the FATF because of the risks outlined above, which are inherent to the rapid implementation without consultation of the R.16.

We would like to recall that there are too few VASP players in Europe and that there is a shortfall in equity capital for these players. The BVC WG therefore considers it essential to preserve European independence in terms of technology and access to the financial tokenization market, to preserve our economy and our jobs.

We would therefore ask the European Commission to implement R.16 in European law with special attention to the following aspects:

- Extend the registration obligation to other activities: crypto-fiat exchange;

- Consider the GDPR when looking at a European implementation of R.16 and make such an implementation compatible and compliant with the GDPR, while avoiding massive data transfers coming from European companies and consumers to other jurisdictions;
- Proactively initiate the fundamental debate on the compatibility of the AMLD and the FATF recommendations with the fundamental rights as outlined in the ECHR and GDPR, in order to provide for more legal clarity;
- Provide a European interpretation of the required identification of the beneficiary "to their best efforts";
- Even if the "best efforts approach" above was retained as the European approach to R.16, consider that R.16 would still ask the originator VASP to '*immediately and securely*' send the information to the beneficiary VASP, and there is currently no way to transmit this information in such a way;
- Try and encourage the development of a European solution to transmit this data as required by R.16 and consider the use of a domestic regime for the European union, allowing for a proportional data delivery on the basis of actual validated suspicion of crimes, rather than automated data broadcasting and retention procedures;
- Coordinate with European Member States to propose a common European reading to the FATF of the difficulties of R.16.

Furthermore, more widely, we would ask the European Commission to proceed in this area with special attention to the following aspects:

- Harmonize the regulation and licensing framework of VASPs between European countries and create a passporting solution in Europe for VASPs registered or licensed in a European country as it is already the case for other financial activities;
- Create a large incentive plan to promote and facilitate the development of a VASP ecosystem in Europe by European players, as a source of employment, competitiveness and sovereignty. Such a plan shall create a positive regulatory environment and help companies to find equity and non-equity financing while compelling the traditional banking system to allow bank access to VASPs and the traditional insurance system to create insurance offers suitable for VASPs.

We welcome your comments and are happy to take any questions you may have.

Sincerely,

Monica Monaco, Secretary General,

Blockchain and Virtual
Currencies Working
Group (BVC WG)

The Blockchain and virtual currencies Working Group

The Working Group is registered in the European Transparency register under number: [635727423661-17](https://www.blockchainwg.eu) and is a member of the European Commission Payment Systems Market Expert Group (PSMEG). Our main aim is to educate European regulators in shaping regulation that will promote innovation in the blockchain and virtual currencies space, while ensuring the protection of consumers and market players. Members include nearly one representative per type of business which exist in the blockchain and virtual currencies space such as wallet providers, virtual currencies exchange platforms, virtual currencies payment processors, market makers, virtual currencies wallet providers as well as companies using the blockchain technology to analyse transactions trails. The following companies are members of the “Blockchain and virtual currencies Working Group” (WG) :

AnycoinDirect
B2C2
Bitcoin.de
Bitflyer
Bitonic
BitPay
Bitso
Bitstamp
CEX.io
Chainalysis
Coingate
Coinhouse
Coinify
Cryptoprocessing
Elliptic
Ledger
LocalBitcoins
Nets
Scorechain
Koban

More information on the Blockchain and Virtual Currencies Working Group can be found on our website: <https://www.blockchainwg.eu>.