Response to the public consultation on Recommendation 16 regarding Payment Transparency initiated by the Financial Action Task Force (FATF)

On May 3 2024, Adan, in collaboration with VerifyVASP whose positions the Association supports, responded to the public consultation launched by the Financial Action Task Force (FATF) concerning revisions to Recommendation 16 (R.16) and its Interpretation (INR.16). This initiative aims to adapt existing standards to technological innovations and changes in business models in the area of payments and financial services. In this context, the objective of this consultation is to ensure that standards remain technologically neutral and adhere to the principle of neutral technology.

The proposed revisions clarify the roles and responsibilities of various actors in the payment chain and enhance the quality of information related to the originators and beneficiaries of payments. Among the suggested changes are also terminological adjustments to better match international payment messages, new clarifications at the start of the payment chain, and measures to ensure the consistent application of R.16 to virtual assets and Money or Value Transfer Services (MVTS). They are designed to align with international messaging standards and legal entity identifiers (LEI), while also incorporating enhanced transparency requirements for card transactions and refining the exemption criteria to better address emerging risks and technologies.

The provided response to the FATF consultation here addresses several points that align well with the primary objectives of enhancing payment transparency and maintaining technological neutrality.

In essence, Adan fully supports VerifyVASP's position in response to the FATF consultation and together supports the measures advocated in the consultation submitted by FATF. Indeed, Adan endorses the proposed limitation of exemptions, recognizing the importance of maintaining consistency and transparency in payments. This approach would ensure better monitoring of transactions while preserving the need for exemptions in specific situations, provided alternative transparency measures can be implemented in a technologically neutral manner.

Additionally, Adan share VerifyVASP's concerns regarding the practical challenges associated with certain aspects of the proposed revision - as explained below, particularly concerning unique personal identifiers and places of birth. We believe a more nuanced approach is necessary to balance data transparency with privacy and protection. Regarding the enhancement of beneficiary data transparency and alignment, Adan supports the need for greater transparency while understanding the reservations expressed about practical challenges. We believe it's crucial to find solutions that achieve these objectives without compromising data security or individual privacy. Lastly and as VerifyVASP, Adan recognizes the fundamental role of international standards (such as ISO 20022) and legal entity identifiers in implementing these revisions.

➔ **Despite potential technological challenges, we are confident that clear adoption of these standards will greatly improve payment transparency and strengthen efforts to combat illicit activities in the financial sector.**

Adan and VerifyVASP are grateful to the Financial Action Task Force (FATF) for allowing the expression of industry players through this consultation and strongly support these revisions that enhance payment transparency while promoting financial inclusion.

VerifyVASP

19 April 2024

Association pour le Développement des Actif Numériques (ADAN)
Delivered via: faustine.fleuret@adan.eu

Dear Ms. Fleuret

Re: Comments of VerifyVASP on the FATF proposed revisions to R.16/INR.16 Executive

Summary

The objective of the proposed revisions to R.16 is to enhance payment transparency while upholding technical neutrality. Discussion items can be summarized as follows: i) limitation on exemptions; ii) expanded data on beneficiaries; iii) alignment of received beneficiary information; iv) definition at the start of a payment chain; v) consistency of R.16 application towards VA and MVTS; and vi) alignment with international standards in messaging and legal entity identifier. We have developed our response under the principles of payment transparency, regulative consistency, compliance efficiency, and financial inclusion.

We support the limitation of exemption under the principles of consistency and payment transparency. Exemption may be retained for exceptional cases where transparency can be secured in an alternative, and technologically neutral manner. Regarding beneficiary data and alignment, we welcome the revision for enhanced transparency. But at the same time, we express concerns about the practical challenges and unintended consequences regarding unique personal identifiers and places of birth. To reflect the payment or value transfer reality in a higher definition and fidelity, we opine to split instruction and funding source information and, thereby, define the payment chain under instruction route while providing a thread to trace back to the source institution and originator. Also, we noted that the alternative funding route could pave a dangerous and unintended path to exclusion and de-risking. We support the consistent application of R.16. However, due to the delay towards R.15 implementation, the majority of institutions are yet to be under sufficient regulatory oversight in the virtual asset sector. Reflecting this reality, we suggest that conducting pre-verification on beneficiaries should constitute a best practice for the ordering institutions to prevent ML/TF exposure and improve compliance efficiency. Implementation of the revision would be highly dependent on the adoption of ISO 20022 and other international standards, including LEIs. While technological challenges will surely cause friction, we opine that the adoption of a clear direction and timeline will contribute towards payment transparency.

Lastly, we observe a concerning gap between the financial sector and abusers utilizing new technologies. Technology should not be allowed to be taken advantage of and monopolized by abusers. We urge the FATF and national regulators to promote adopting new weapons and initiatives in the war against ML/TF. No fresh path to effective ML/TF risk mitigation can be found without the aid of new technology.

Sincerely,

Azman Hamid

Nor Azman Bin Hamid
General Counsel

Chia Shih Yun

Shih Yun Chia
CEO

VerifyVASP

Comments of VerifyVASP on the proposed revisions to R.16/INR.16

a. Retaining the existing exemption for purchase of goods and services, subject to additional transparency requirements (paragraph 4 (a) of INR.16)

Questions for consultation on the card exemption

Q.1 - Do you support FATF's proposal above? If so, which option will be better and why? If you do not support FATF's proposal, please explain why. Are there any appropriate alternative proposals to ensure transparency, adequate AML/CFT controls and level playing field while minimising the unintended consequences?

We support FATF's proposal on the limitation of the card exemption. As noted in the explanatory memorandum, a clear distinction between 'purchase of goods or services by cards' and 'transfer of money' is virtually impossible in reality. With the existence of relatively efficient marketplaces, any goods or services purchased by cards can be converted back to money. Recent developments in online marketplaces and the emergence of virtual assets (online money) as a store of value and/or medium of exchange have greatly reduced the distinction between 'purchase' and 'transfer of money'. This distinction will be further blurred with the increased adoption of virtual assets, various types of cards, peer-to-peer marketplaces, cross-border and online card transactions. For this reason, we opine that R.16 needs to be applicable to card transactions in general, unless there is a very clear reason for its exemption. Following the same logic, we welcome the collection and submission of additional data points (the name and location of issuing and acquiring financial institutions) for the purpose of unambiguous identification of card holders and merchants where necessary.

Following the rationale above, we think Option 2 (removal of withdrawal or purchase of cash or a cash equivalent from the R.16 exemption) is a better option. Otherwise, purchase of so-called stablecoins with prepaid cards will be out of R.16 scope, thereby failing to identify the originator and beneficiary of such money or value transfers, which would be against the principle of consistency (same activity, same risk and therefore same regulatory outcome).

Q.2 - Are there any important aspects that the FATF needs to consider in finalising the revisions to R.16 and working on FATF Guidance on payment transparency in order to facilitate consistent implementation of FATF Standards between jurisdictions, based on considerations such as feasibility of the proposals, timeline of implementation and mitigation of unintended consequences such as disproportionate impact on cost, financial inclusion, and humanitarian considerations?

Data collection and submission obligations (the name and location of the issuing and acquiring financial institutions merchant) in addition to card numbers could have a disproportionate impact on smaller and offline merchants, especially in developing countries, which is against the principle of financial inclusion. Depending on existing messaging protocol of cards and terminal devices at the point-of-sale, additional data collection and submission may not be readily available without replacing the current messaging protocol, physical cards or terminal devices. We believe this limitation needs to be considered in the timeline of revision to avoid unintended consequences.

It could be relatively easier to collect and submit additional data in case of online card payments. Online card payments are being processed by a relatively small number of payment processors and the messaging standards

used by all connected merchants can be updated remotely. If online card payments account for a large portion of known ML/TF cases, then a viable alternative could be to apply a proposed revision for online card payments first, providing additional lead time for the offline merchants and financial institutions providing card payment services to them.

Q.3 - Which data fields in the payment message could be used to enable financial institutions to transmit the information on 'the name and location of the issuing and acquiring financial institutions' in a payment chain? If appropriate data fields or messaging systems are not currently available, how could they be developed and in what timeframe?

It is ideal to use the ISO 20022 standard for machine-readable and streamlined common messaging structures. But given that the majority of existing card payment messaging standards currently in place are based on various legacy versions of ISO 8583 standards, mixed use of both standards (ISO20022 and ISO 8583) would be inevitable at least for a few years.

In case of ISO 8583, the name and location of the acquiring financial institution can be included in MTI x1000 (Authorization Response) or x2000 (Acquirer Financial Request). More specifically, data fields 19 (type n 3) 'acquiring institution country code' and data field 32 (type n ..11) 'acquiring institution identification code' could be used. Similarly, it would be ideal to use a pre-defined data field for issuing financial institutions. But legacy versions of ISO 8583 do not have specific fields for issuing financial institutions, and some financial institutions use fields reserved for private use. In such a case, it might be necessary to use data fields reserved for ISO use for issuing financial institutions upon necessity.

Additionally, we support the Global Legal Identifier Foundation (GLEIF)'s proposal to expand the GLEIF-SWIFT mapping partnership to include all BIC types. SWIFT is the registration authority for the ISO 9362 (BIC) standard for identification of institutions within the financial services industry. BICs are the most common routing keys and can serve to transmit information on the name and location of the financial institution's business unit involved in the payment chain. Expanded mapping between GLEIF and SWIFT would allow all parties involved in payment messages or receiving data associated with payment messages to move seamlessly from the BIC as a reference to the involved business units of the issuing and acquiring financial institutions to the LEI as a reference to the legal entities associated with these business units, which in turn would enhance screening of ISO 20022 payment messages.

Application of the exemption to different card types

Q.4 - Do you support the FATF's proposal to apply the amended card exemption equally to credit, debit, and prepaid cards? If not, why? Are there any appropriate alternative proposals? In terms of the potential differences in AML/CFT risk profiles and mitigation measures in different types of cards such as credit, debit, and prepaid cards, are there any aspects that FATF should pay due attention in finalising revisions to R.16 and in developing the future FATF Guidance on R.16? If so, what are they?

We support the FATF's proposal to apply the amended card exemption equally to credit, debit, and prepaid cards on the principle of consistency (same activity, same risk, same regulatory outcome).

Q.5 - Considering that the current exemption extends to credit, debit and pre-paid cards, are there any other similar means of payment that should be included in the card exemption for the purchase of goods and services? What are examples of those means of payment, and why should they be included in the exemption?

In the principle of consistency, we opine that other means of payment that share the basis of card exemption should be included (i.e. closed systems, in which the originator and beneficiary are customers of financial institutions, which in turn are contractually obligated by the payment network to adhere to certain AML/CFT and sanctions compliance measures). Common facilities falling under the category of 'other means of payment' would be stored value or e-money services. Usually, these services are regulated activities under the supervision of a financial regulator with a prescribed cap on the total stock (amount) and flow. As originator and beneficiary (merchant) belong to the same financial institutions, it constitutes a closed loop in terms of KYC/CDD and payment information flow. In most of the cases, its usage is limited to certain type of merchants (food delivery, ride hailing, etc.), showing the characteristics of a further closed network. Merchants of these services are mainly small to medium offline businesses, an important segment for financial inclusion, and are customers of financial institutions. In some regions, stored value or e-money facility could be the only viable payment option where physical distribution of cards is commercially not viable, dangerous or culturally not feasible (e.g. gender equality, religious or other social constraints, etc.). In this regard, we opine that such services (stored value or e-money business) share the basis of prepaid card exemption and subsequently, needs to be exempted for consistency and inclusion.

R.16 and INR.16 need to be future-proof. Depending on the frequency of R.16 and INR.16 updates, we may take a more inclusive stance on the exemption while maintaining consistency. If the key rationale of the card exemption is that i) both originator and beneficiary are customers of financial institutions; and ii) both originator and beneficiary belong to the same informational network (card network) adhering to certain AML/CFT and sanctions compliance measures, we can adopt the same regulative rule exemption to the same activity. Besides stored value or e-money aforementioned, purposeful or merchant-bound money controlled by a financial institution can share the rationale and thus, fall into the exemption list. In this regard, the terms "a credit or debit or prepaid card" can be substituted by "a credit or debit or prepaid card or other means of payment or value transfer facilitated by a financial institution between its customers.".

Scope of "withdrawal or purchase of cash or a cash equivalent"

Q.6 - Should R.16 apply to cash withdrawals and purchase of cash or a cash equivalent? If so, should it apply to withdrawals using credit, debit, and pre-paid cards in the same way, or be differentiated according to card type? Should it apply only to withdrawals above a threshold and if so, what is the appropriate threshold?

We opine that R.16 should apply to cash withdrawals and purchases of cash or a cash equivalent in the same way to credit, debit or pre-paid cards. The listed cases are in B.4. Option 2 is, by nature, the payment or transfer of value rather than the purchase of goods or services. Hence, same activity, same risks, same regulatory outcome or rules.

In our opinion, there will not be much benefit of applying a *de minimis* threshold of USD/EUR 1,000 for domestic withdrawal or purchase of cash or a cash equivalent. Private sector participants will need to establish additional systems to comply with R.16 revision once it is mandated by national regulators anyway. Calculating the applicability (regarding *de minimis*) will only add an additional layer of complexity without clear benefits. The

application of *de minimis* could be abused by structuring multiple transactions or could lead to additional development specifications on financial institutions. Even in the case of Virtual Assets and Virtual Asset Service Providers, the FATF Guidance suggests Travel Rule obligations under *de minimis*, although the verification of the information shared may not be required.

Q.6bis Do you support the FATF's proposed treatment of domestic cash withdrawal? Are there situations in which exemptions should apply (other than domestic withdrawals by a beneficiary from ATMs of financial institution holding its account, in which case R.16 has no applicability)? Are there any important aspects that FATF needs to consider in terms of implementation of applying R.16 to withdrawal or purchase of cash or a cash equivalent?

We opine not to distinguish between domestic and foreign cash withdrawals or purchases of cash or a cash equivalent. Cash can fly cross-border, and different treatments would only complicate the system without benefiting its purpose. As we support not applying *de minimis*, domestic and foreign transactions should also not be treated differently.

[Suggestion] para 4(a) - *mark up from Option 2*

Any transfer that flows from a transaction carried out using a credit or debit or prepaid card or other means of payment or value transfer facilitated by a financial institution between its customers for the purchase of goods or services from merchants, so long as the unique identification number of the originator, including the credit or debit or prepaid card number, as well as the name and location of the issuing and acquiring financial institutions [footnote 47], accompanies all transfers flowing from the transaction.

However, Recommendation 16 does apply in situations:

- when a credit or debit or prepaid card, or other means of payment or value transfer aforementioned is used to effect a person-to-person payment or value transfer; or
- when ~~a credit or debit or prepaid card is~~ used to make a ~~cross-border~~ withdrawal or purchase of cash or a cash equivalent~~; or~~
- ~~when a credit or debit or prepaid card is used to make a domestic withdrawal or purchase of cash or a cash equivalent with a value over USD/EUR 1000~~

Q.7 - What should be included in the scope of 'cash equivalent'? What aspects regarding the scope of 'cash equivalent' should be further clarified? Should such scope be defined in the standards or clarified in the future FATF Guidance?

To achieve regulatory intent, the term 'cash equivalent' needs to include any asset that could be used as the medium of payment or value transfer. In a sense, the definition should be different from the term used in accounting and should not be confined to the similarity to cash itself. In reality, any asset tradable in a relatively efficient secondary marketplace could be used as a cash equivalent. It could be a commodity, treasury bill, virtual asset, or even luxury bag or watch.

Hence, it is impossible to list all assets to capture circumventive activities. Rather, we opine it is more realistic to focus on behavior, which financial institutions should monitor, together with the examples of representative cash equivalents. In such regard, we suggest defining 'cash equivalent' broadly as 'any asset which is being used for the purpose of payment or value transfer, including bonds, debentures or other securities, commodities, virtual assets, or any other digital tokens, and urge financial institutions to monitor transaction behavior in this context.

c. Improving the content and quality of basic originator and beneficiary information in payment messages (paragraph 7 of INR.16)

Q.8 - Would stakeholders support FATF's approach and view that the proposed amendments will improve the reliable identification of the originator and beneficiary and increase efficiency? Which of the two options set out above for the proposed revisions in paragraph 7 would stakeholders prefer and why? To what degree is the customer identification number, as set out in paragraph 7 (d), useful to identify the customer? Are there any other issues or concerns in this regard? Are there any important aspects where the FATF needs to provide more granular advice in the future FATF Guidance in order to facilitate effective and harmonised implementation of the FATF proposal?

We support the FATF's approach to standardizing information and enhancing data quality. The proposed amendments will improve reliability and efficiency of identifying the originator and beneficiary for the purpose of sanction screening by reducing false positives and will contribute to other surveillance mechanisms for AML/CFT and market abuse in general.

We encourage the adoption of Option 1, suggesting asymmetric mandatory information elements between the customer of a financial institution and the beneficiary, for the purpose of maintaining data quality and promoting financial inclusion. For Option 2, we opine that the friction outweighs the potential benefit.

The draft revision can be summarized in the table below where added elements are underlined.

Originator Information	Beneficiary Information
Full name	Full name
Account number where such an account is used to process the transaction. In the absence of an account, a unique transaction reference number, which permits traceability of the transaction	Account number where such an account is used to process the transaction. In the absence of an account, a unique transaction reference number, which permits traceability of the transaction
Address or, in the absence, the country and town name	Address or, in the absence, the country and town name
If natural person, one of - national identification number - unique official identifier - customer identification number - date and place of birth	(only for Option 2) If natural person, one of - national identification number - unique official identifier - customer identification number - date and place of birth
If legal person, one of connected - BIC - LEI - unique official identifier	If legal person, one of connected - BIC - LEI - unique official identifier

Paragraphs 20 and 21 of the draft revision of INR.16 require the beneficiary institution to check the alignment of the beneficiary information received from the ordering institution against the beneficiary information held in the beneficiary institution. Also, in case the beneficiary information it received is not aligned with the information held in the beneficiary institution, the draft revision requires a beneficiary institution to adopt risk-based policies

and procedures of execution, rejection or suspension as well as appropriate follow-up action. We support this added requirement of beneficiary institution on the alignment of beneficiary information (received versus held) and developed our opinion on Q.8 in this regard.

We are of the opinion that Option 2 (requiring the ordering institution to obtain and submit a unique identifier or the date and place of birth of the beneficiary) could result in unintended consequences of conflict with personal data protection regulations, personal data breaches, evasion of financial institutions and financial exclusion.

Unique personal identifiers are highly sensitive personal data protected by various personal data protection regulations around the world. A financial institution may not have difficulties collecting such information from its customers. But the customer will have serious difficulties collecting such unique personal identifiers from a third-party beneficiary upon a payment or value transfer. If there are specific requirements for collecting others' unique personal identifiers, it may not even be allowed for an originator to collect such information in the context of the personal data protection regulations of the originator's jurisdiction. In addition, depending on the personal data protection regulations of the beneficiary's jurisdiction, the unassuming originator or ordering institution may violate the regulations of the beneficiary's jurisdiction, unintendedly. As the beneficiary institution is expected to align the collected unique personal identifier against the information it holds, harmonization with global personal data regulations would be a pre-condition to implementing this revision, and it could result in a serious delay in its implementation.

Additionally, unique personal identifiers are sensitive information for all parties. A beneficiary may have certain reservations about sharing such information with the intended originator and ordering institution. To avoid sharing sensitive information, an intended beneficiary could explore alternative options, including virtual assets or other means of payment or value transfer, and it could lead to the exact opposite outcome versus the intention of this revision.

Even in cases where there is no restriction or friction in obtaining and submitting the unique personal identifier of the beneficiary, given the number and frequency of payments or value transfers, the exchange of such sensitive personal data between 'originator and beneficiary (to submit such information to the ordering institution)' and between 'ordering institution and beneficiary institution' could result in a massive breach of personal data. By making the request for such sensitive information customary, illicit actors could capitalize on this as a new opportunity to seek out unique personal identifiers. For example, a voice phishing scammer may approach an unassuming person, asking for their unique personal identifier under the pretense of a false payment or value transfer to their account. Once a unique personal identifier is leaked to an illicit actor, the damage from it could outweigh the benefit of including such information in payment or value transfer messaging.

After all the complications and side effects of obtaining and submitting a beneficiary's unique personal identifier, the additional probative value from it is very limited. The biggest potential value of it would be an automated check on the consistency between the collected beneficiary information and the information held by the beneficiary institution. But this objective would fail in cases where different unique personal identifiers might be used (e.g. passport number vs national ID number). Also, there is less sensitive information to verify the consistency, including full name and address, without wreaking havoc on personal data protection or attracting scammers. Regarding the name screening of the beneficiary conducted by the ordering institution, the unique personal identifier of the beneficiary will not add much value as unique personal identifiers of illicit actors, including designated entities or individuals are not known, in most cases.

'Date and place of birth' could be a less sensitive alternative. But in our observation, many financial institutions do not collect 'place of birth' from their customers. In such cases, even if a beneficiary institution receives the information, there's no information to check the alignment against it. Unlike addresses, collecting document evidence of place of birth is not easily available in all countries. In certain cases, the customer of a financial institution may need to physically visit the relevant governmental office of the place or province of birth for documentary evidence, which adds significant friction. For certain segments of customers, it won't be feasible to obtain the document due to the limitations of time and/or cost associated with it. Illicit actors' place of birth is not readily available, although it is more available than their unique personal identifier. This reality further limits the probative value of the additional data, resulting in the friction outweighing the potential benefit.

'Date of birth' alone (without place of birth) could be a viable option. Even if date of birth is personal data, it is not a unique personal identifier. Also, the majority of financial institutions would collect the dates of birth of their customers. Getting documentary evidence is fairly straightforward in any country. It has a more standard format by nature, which allows for automated verification, contributing to efficiency. It could still be a concern to share date of birth to a third party just because that party needs to effect a payment or value transfer. But compared to unique personal identifier or place of birth, it is a much better and pragmatic alternative. In regards to the probative value during name screening, date of birth (usually year of birth) could be effective data to easily filter out false positives. If a concerned illicit actor is in their 40s, simply knowing that the beneficiary is in their 20s (even if the name is same) would be reasonable ground to dismiss the suspicion.

Another angle to consider is that the originator will be gathering beneficiary information (from direct communication with the beneficiary), and acting as the first gatekeeper. The originator has limited ability to detect any misrepresentation in unique personal identifier (e.g. passport number, national ID number) or place of birth. But it would be reasonably possible for the originator to detect misrepresentation in full name, address and date of birth (at least rough year of birth) as these are relatively recognizable data publicly. For the purpose of verification or alignment, we are of the opinion that utilizing public data results in better adoption and higher transparency.

For this reason, between Option 1 and 2, we prefer Option 1. If Option 2 were to be implemented, then we propose to use date of birth only as an additional information element for the beneficiary.

We also suggest that the Legal Entity Identifier (LEI) should be encouraged as a global, readily available, digital standard for identifying the originator and beneficiary legal person. Compared to the other identifiers mentioned in 7(e), only the LEI has all the required features that will enable transparent party identification in cross-border payments.

d. Addressing transparency in case of virtual IBANs and other similar account naming conventions (paragraph 7(b), footnote 1 of INR.16)

Q.9 - Do stakeholders have any views on the suggested approach to ensure more transparency about the location of originator and beneficiary accounts? Are there any issues or concerns?

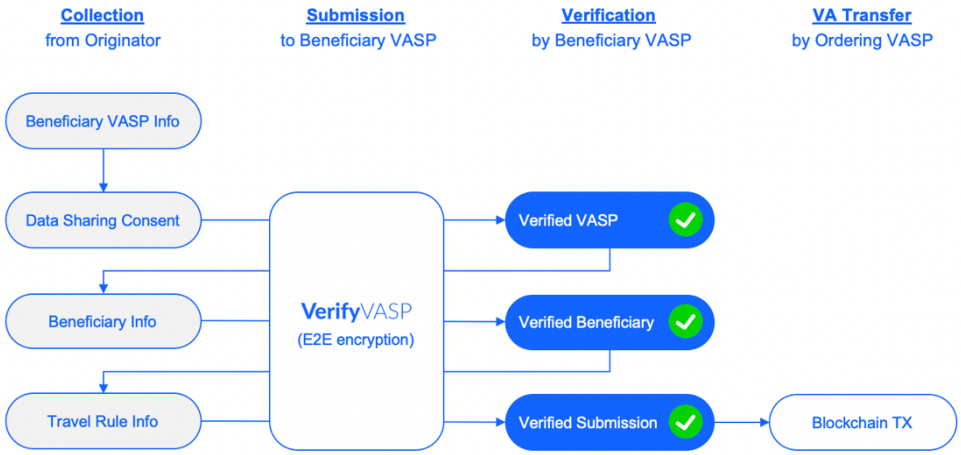
We have no issues or concerns on this topic.

e. Obligations on beneficiary financial institutions to check alignment of beneficiary information in payment messages (paragraph 20 and 21 of INR.16)

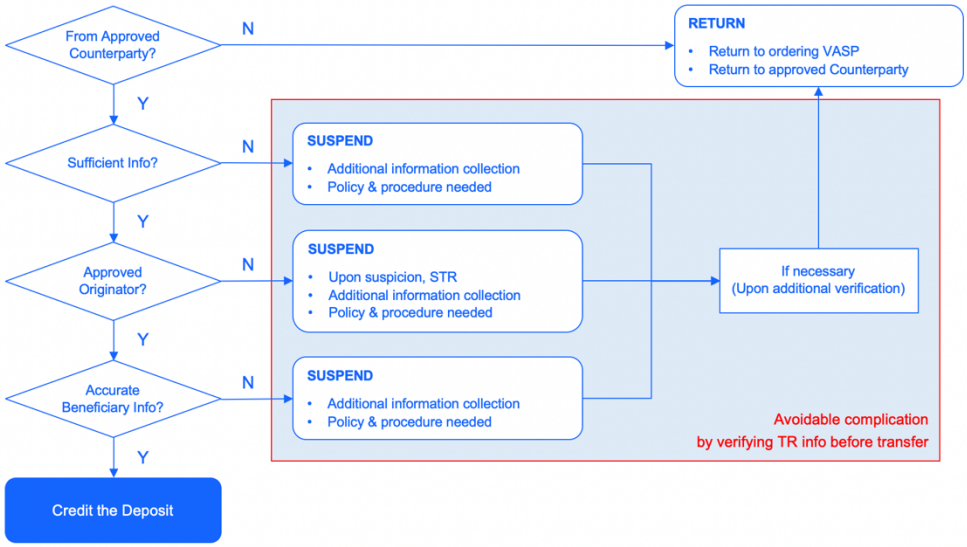
Q.10 - Do stakeholders support the FATF's proposal? If not, why? Will the proposed obligations help financial institutions in better addressing their financial crimes risks? Does the term "aligns with," together with the risk-based provisions in paragraph 21, create a clear and sufficiently flexible standard? What are potential unintended consequences of this proposal if any? In terms of how financial institutions can meet these requirements more effectively and efficiently, what kind of guidance and information should the future FATF Guidance include? If financial institutions have already implemented these checks, what are the current best practices of implementing the proposed requirements that could be introduced in the future FATF Guidance?

We support the FATF's proposal on mandating alignment checks.

As the largest R.16 (Travel Rule) solution in the world in terms of the numbers of verifications undertaken in the context of virtual assets, we already support our member VASPs to verify declared beneficiary information (name and 'date of birth' additionally, for enhanced risk mitigation measure) against the beneficiary VASP prior to effecting a virtual asset transfer, as illustrated below.

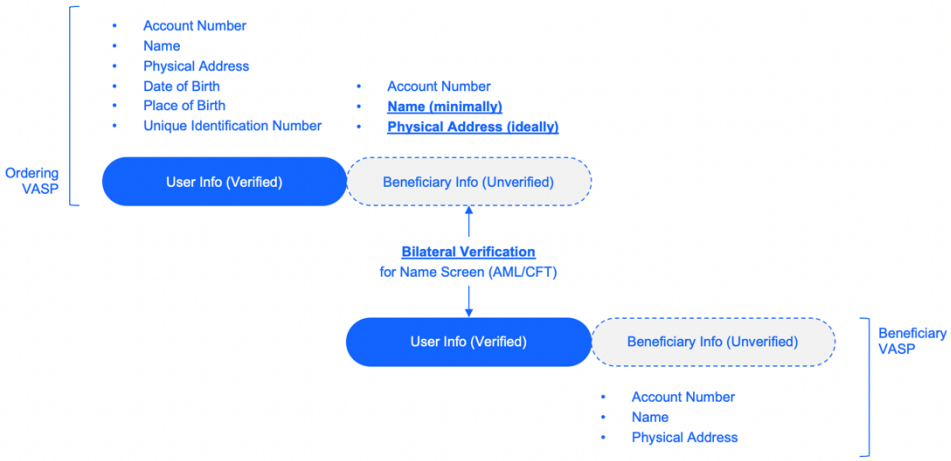


The verification is based on a real-time JSON API integrated between our members. The average time to verification is 0.168s (2024 March). Due to the instantaneous verification, we have not faced any friction while processing more than 7 million verifications so far during the last 2 years. Considering the beneficiary information is verified before the value transfer; beneficiary institutions have not faced many complications when verifying the alignment unless there is a deposit made outside of our protocol. Even if it was not mandated to verify the beneficiary prior to the virtual asset transfer, we deemed pre-TX (transaction) verification to be necessary as beneficiary VASPs can span a wide spectrum of forms (licensed, registered, unregulated, regulated but under weak regulatory oversight, etc.). To use a common example, this workflow avoids any possibility of accidentally effecting virtual asset transfers to a beneficiary with an unverified name (thus it becomes impossible to send a Bitcoin to Mickey Mouse despite having all travel rule data fields completed). With this background, we have gathered experience during the last 2 years on what happens if a beneficiary institution (in our context, a beneficiary VASP) starts to check alignment (in our context, exact match verification).



As illustrated above, from the moment of checking alignment, there will be cases of 'not aligned deposits. Beneficiary institutions need to prepare policies and have procedures in place to process such cases in a timely manner. The process would include the collection of additional information, additional check or verification, and the return of the funds, or filing STR. We note that guidance is needed as to whether a beneficiary institution needs to apply R.16 to the return transaction (in cases of misalignment). Such cases can be avoided by the ordering institution verifying the beneficiary prior to the payment or value transfer. But due to legacy infrastructure and policy, this ideal workflow may not be feasible in all cases.

We opine that 'alignment' is a fairly reasonable term, as an exact match could result in too much friction. For example, a minor difference in name (e.g. position of middle name, special characters, space between words, even uppercase & lowercase differences) can be dismissed even if it does not result in an exact match. Similarly, address matches may show similar nuances due to the lack of uniformity in the name of the town or country, even if participating institutions are communicating in accordance with the protocol of ISO 20022 and checking against the mandatory fields only, especially in the case of cross-border payment or value transfer.



As illustrated above, Travel Rule information consists of 2 blocks. Customer information (verified) and counterparty information (unverified). Usually, the customer information is being verified by the financial institution. But in the case of counterparty information, there is a lack of verification, resulting in limited transparency in the chain of payment or value transfer information.

There are 2 options to establish transparency in the payment or value transfer chain. Option 1 is to mandate that the beneficiary institution verify (or check alignment with) the beneficiary information it receives against the beneficiary information held within. Option 2 is to mandate that the ordering institution verify the collected beneficiary information against the beneficiary institution prior to effecting the payment or value transfer. In Option 2 the beneficiary institution will also verify the received beneficiary information, establishing the four-eyes principle as best practice. There are pros and cons of the two approaches as summarized in the table below.

	Option 1 (post-verification)	Option 2 (pre-verification)
Verification Obligation	Beneficiary institution	Ordering & beneficiary institution
Verification Timing	After payment or value transfer	Before payment or value transfer
Verification Basis	Intra-institution data reconciliation	Inter-institution data reconciliation
Time to Verification	Few hours – days Common expectation on cross-border TX	Instant Originator expects response in real time
Efficiency	*Low* In case of misalignment, beneficiary institution needs to reverse or return the transaction	*High* Reduced cases of misaligned beneficiary details as the screen is being conducted pre-transaction
Name Screen Effectiveness	*Low* Ordering institution conducts name screen with unverified beneficiary details	*High* Ordering institution conducts name screen with verified beneficiary details
Payment Transparency	*Low* There is no guarantee that ordering institution holds accurate beneficiary information for a transaction	*High* All participating institutions hold accurate information for originator and beneficiaries for all transactions
Technical Difficulty	*Low* No technical integration required between institutions for the purpose of beneficiary verification	*High* Technical integration is required between institutions and it should enable instant verification of the beneficiary

As summarized, Option 2 is far preferable to Option 1 in terms of efficiency and transparency. This is even more prevalent when it comes to policies and procedures of the beneficiary institution. For example, in case of VASPs (Virtual Asset Service Providers), due to the delay and varying level of regulatory oversight regarding R.15 and R.16, beneficiary institutions may not be very reliable. In such context, only Option 2 allows the ordering institution to conduct effective name screening on the beneficiary before effecting the transfer of virtual assets. Without Option 2 in a virtual asset context, an ordering institution could be conducting beneficiary name screening with inaccurate information, and the beneficiary could not be checking the alignment or accuracy of the received beneficiary information.

However, Option 2 poses a much greater technological challenge than Option 1. Beneficiary verification prior to a payment or value transfer requires technical integration between the ordering and beneficiary institutions. Also, as the ordering institution will be required to inform the originator of the result of the beneficiary verification instantly (for instance, the originator can be waiting at the bank branch), and the beneficiary institution needs to respond to the verification request in real-time.

Due to this technical challenge, even if Option 2 is ideal, mandating it could lead to decreased financial inclusion as not all financial institutions could implement such technical protocol supporting real-time beneficiary verification. For this reason, we opine that Option 1 could be a better option for traditional financial institutions in a first instance. But it is worth noting that there is residual risk in this option: an ordering institution can conduct name screening with unverified beneficiary information. For this reason, we think there is an opportunity to promote Option 2 in the virtual asset industry as a greenfield initiative. Also, wherever feasible for financial institutions, beneficiary verification prior to the payment or value transfer needs to be encouraged for improved transparency and efficiency.

f. Definition of payment chain (paragraph 23)

Q.11 - Do you agree with the issue that FATF has identified with respect to the start of a payment chain and support FATF's approach to address the issue? The proposed revision (paragraph 23 of INR.16) has two options on whether the payment chain should begin with the instruction by the customer (Option 1), or with the funding (Option 2). Which of the two options would stakeholders prefer for the start of the payment chain and why, also considering the response to question 12 for consultation set out below? What are the aspects where more granular guidance in the future FATF Guidance could be helpful?

We agree with the issue that the FATF has identified. It is necessary to establish payment or value transfer transparency across the whole chain, rather than leaving participating financial institutions blinded as to who is the source originator and who is the ultimate beneficiary.

We support Option 1 (instruction route option) more than Option 2 (funding route option). While both options result in the same result in most of the cases, it shows a different result if the originator uses MVTS to transfer funds from their funds kept in a financial institution other than the MVTS via debit payment. In such a case, the MVTS is 'the institution receiving an instruction' and the other financial institution is 'the origin of the funds.

Even in the case of Option 1, proposed footnote of paragraph 7(b) will require the ordering MVTS to include the information of account number and financial institution where the origin of the funds is held in the payment message it submits to the beneficiary MVTS. So, we developed our opinion based on the perspectives of the financial institution which is the origin of the funds (Bank A in the Explanatory Memorandum page 9) and intermediary institution (Bank B).

The benefit of Option 2 is that it provides additional information to Bank A (financial institution holding originator's funds) and to Bank B (financial institution where the ordering MVTS is holding an account). But as Bank A does not collect information on the beneficiary nor beneficiary institution from its customer, it needs to receive such information from the ordering MVTS F. Subsequently, Bank A will submit R.16 information to Bank B, then ordering MVTS F. R.16 information will traverse MVTS F (information collector) → Bank A (ordering institution) → Bank B (intermediary) → MVTS F (intermediary) → MVTS G (intermediary) → Bank D

(intermediary) → Bank E (beneficiary institution) forming a partial circular reference loop. In such an architecture, we expect potential complications of i) inefficiency, ii) accountability, and iii) exclusion and de-risking.

Under Option 2, we have a circular reference of the information MVTS F collected between Banks A, B and MVTS F. This could lead to redundant name screens in multiple financial institutions. As beneficiary information is not even verified, the inefficiency may outweigh the benefit. For example, if customer X instructs MVTS (a customer of Bank Columbia) to send funds to Mickey Mouse in Bank Disney from their funds kept in Bank Sony, then Bank Sony, Bank Columbia (as an intermediary institution, out of prudence) and MVTS will conduct name screening on Mickey Mouse, which is not even verified information, resulting in inefficiency.

Having R.16 information may also create accountability. Upon R.16 information sharing, Bank A may be accountable for transferring the funds of X (its customer) to Y (not their customer, also the cross-border transfer is not under their control or by the instruction of their customer). Similarly, Bank B may be accountable when X (originator) is not their customer and the cross-border transfer is not initiated by them. Even if MVTS F and G are the parties accountable for screening and monitoring, this shared accountability could result in no one having actual accountability. Depending on foreign currency exchange transactions or other related regulations, additional information Bank A and B receive may induce regulatory complications as there is a discrepancy between the information (cross-border transaction) and the actual transaction they perform (domestic transaction). For example, Bank A may be subject to separate reporting obligations regarding a purported cross-border transaction, but without the necessary details as they are not the party initiating the cross-border transaction.

Lastly, unlike any other form of R.16 information submission, the information sharing from MVTS F to Bank A needs to be a pull-payment message (or other workable mechanism), as the sharing should be triggered by the request of Bank A. Unless both bank and MVTS are high-capacity financial institutions, this new type of payment message protocol is unlikely to be established. More critically, MVTS F will need to establish a pull-payment message or other mechanism with *all* potential banks holding originators' funds. As such a messaging protocol cannot be established without engaging the support of banks holding originators' funds, this challenge is prohibitive and may result in serious exclusion and de-risking behavior exacerbated by an element of competition (Bank A vs MVTS on cross-border payment or value transfer). Given the fact that MVTS contributed to bringing a significant portion of unofficial cross-border transactions into the realm of regulated financial services, the risk of exclusion and de-risking could result in a significant setback in certain geographical regions or customer segments, which would go against the intent of the FATF.

With the aforementioned rationale, we believe Option 1 is better in reality. Regarding the residual risk of fragmented payment messaging, we believe the proposed footnote of paragraph 7(b) could mitigate it to a certain extent (we have a proposed revision on footnote). Still, there would be residual risks. But it would be better to mandate MVTS to strengthen its capability in screening and monitoring, rather than sharing and splitting the accountability. Bank A and Bank B should assess the risk associated with their customer's (X and MVTS F, respectively) activities. Making a financial institution accountable for their customers' activities would be a more straightforward and clear direction, as long as the additional footnote of para 7(b) can establish a minimum thread to trace back for unambiguous identification of the originator and the financial institution holding the funds of any payment or value transfer.

Q.12 - Do you support the idea of adding footnote 2 of para 7(b) if FATF adopts option 1 above in Q.11? Can the ordering financial institution obtain this information, populate the payment message, and execute the payment? How can

this additional information be included in payment messages, e.g., the ISO20022 message? If appropriate data field or messaging system is not currently available, how could this be developed and in what timeframe? Is this footnote clear enough, especially in terms of when and in which cases this requirement applies? Are there any important aspects where the FATF needs to provide more granular expectation in the future FATF Guidance paper?

We support the idea (rather than the exact wording itself) behind adding footnote 2 to para 7(b) together with Option 1, as described in our response above. We have also added a proposed revision to the footnotes below, separately.

The ordering institution (MVTS F, in the Explanatory Memorandum page 9) receives instructions from Customer X. The MVTS F will be able to receive the information of the account number and financial institution, which is the origin of the funds, together with the payment or value transfer instructions. As this is a communication between Customer X and the MVTS F, not involving any other financial institution, obtaining the information during the provision of MVTS F service will be fairly straightforward, especially compared to Option 2 (a pull-payment message or other workable mechanism between financial institutions). The reliance on the information declared by Customer X can be questioned. But in most of the cases, MVTS F will be able to verify account number and the name of Bank A by monitoring its banking transaction information on Bank B, where necessary.

We do not have visibility regarding the availability or timeline of including such additional information into ISO 20022 messaging, as it would be dependent on the participating financial institutions.

Considering the speed of developments in the payments or value transfer sector, allowing a financial institution to add information about the source account number and financial institution information, which is not the ordering institution itself, is necessary to maintain the robustness of R.16 implementation. Besides MVTS, there could be other forms of payment of value transfer services acting as the ordering institution (instruction of payment or value transfer without having an originator as their customer or holding their fund). Rather than simply extending the definition of payment chain back to the source of funds, causing the complications aforementioned, dropping the implied assumption of 'ordering institution holds originator's funds' and allowing separation of 'ordering (instructing) institution' and 'source of the funds institution' would be more flexible. The separation will result in higher definition and accuracy in payment information, correctly reflecting the true nature of a payment or value transfer chain.

Following this rationale, we have revised the footnotes of paragraph 7(b) to ensure uniformity in payment information regardless of the location of the origin of the funds.

[Suggestion] para 7(b)

the account number [*footnote 1] of the originator and beneficiary where such an account is used to process the transaction. In the absence of an account, a unique transaction reference number should be included, which permits traceability of the transaction [*footnote 2];

[*footnote 1] The account number or the associated payment message data should enable the institutions and authorities referred to in paragraph 1 to identify the financial institution and the country where the account holder's funds are located.

[*footnote 2] In cases where the origin of the funds is a financial institution other than the ordering financial institution, the account number, the name, and the country of the financial institution that is the origin of the funds should be included.

g. Conditions for net settlement (paragraph 24)

Q.13 - With the clarity on the payment chain (paragraph 23) and paragraph 24, do stakeholders observe any remaining risks associated with net settlement that should be addressed in the R.16/INR.16 amendments? Are there any aspects where FATF should provide more granular expectation in the future FATF Guidance?

With the clarity on the payment chain (paras. 23 and 24), together with the expanded scope specified in para. 22, we don't have any remaining major concerns associated with the net settlement exemption for R.16 exercise.

As detailed out in our response to Q.11, we opine that it is more effective to oblige financial institutions focus on screening and monitoring the behavior of their customers, rather than splitting accountability across a payment chain. Against the backdrop of the competitive element (Bank A vs MVTS), it is more effective to strengthen screening and monitoring capabilities of MVTS to address the residual risks regarding net-settlement rather than paving a potential path to financial exclusion and de-risking.

h. Financial inclusion, de-risking and other policy consideration such as cost and speed

Q.14 - Do stakeholders have any views on the proposed revisions to R.16/INR.16 from a financial inclusion perspective, including potential impact on account-opening policy and procedures of financial institutions, and humanitarian considerations? Which, if any, specific proposals raise particular concerns? Are there any alternative approaches or mitigating measures in case of such concerns?

Yes, we have concerns in terms of competition (bank vs. MVTS), financial inclusion, and humanitarian considerations. Our concerns have been incorporated into our responses to each question.

i. Impact on other FATF Recommendations

Q.15 - When and how the R.16 revision applies to the virtual assets (VA) sector will be considered separately by FATF. If you are aware of any technical difficulties or feasibility challenges in applying this proposed revision to the VA sector, please specify. FATF will welcome proposals on how to address those difficulties and challenges, if any.

As the world's largest R.16 solution for the VA sector, we (VerifyVASP) have developed our response to this draft revision on a technology-neutral basis. In other words, we don't see any technical difficulties or feasibility challenges in applying this proposed revision (assuming our feedback is considered) to the VA sector.

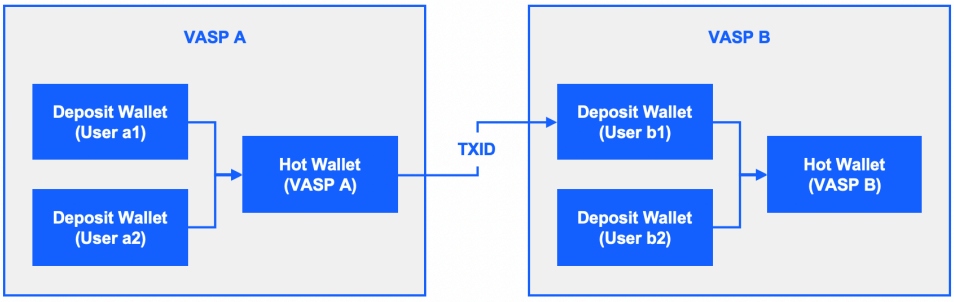
To the contrary, considering the inherent risks of the VA sector (the instantaneous and borderless nature of VA transfers and the delayed and varying levels of R.15 and R.16 implementation), we opine that the VA sector needs to adopt a stricter policy, as reiterated in our response to Q.10. The table below summarizes the suggested policy.

	Draft Revision	Suggestion for VA Sector
Verification Obligation	Beneficiary institution	Ordering & beneficiary institution
Verification Timing	Post transaction	Pre & post transaction (four-eyes)
Verification Level	Alignment	Exact match
Enhanced Risk Mitigation	N/A	First-party only

The key suggestion is to encourage pre-verification by the ordering institution prior to transferring the VA. We will explain the rationale here from another angle (in addition to the rationale described in the response to Q.10). From the moment of R.16 implementation, it is inevitable that a VASP will receive VA transfers (via blockchain), which are lacking the required R.16 information. The FATF guidance or local regulations do not specifically prescribe requirements for the Travel Rule non-compliance return policy. This leads to VASPs adopting various practices for return policies. Key considerations on a return policy are:

a) where to return to;
b) who to return to;
c) applicability of Travel Rule compliance

Most VASPs operate aggregated wallets (usually, hot wallets) to process multiple users' withdrawal requests. While deposit wallet addresses are unique to each user, withdrawal wallet addresses ('from' address in blockchain transaction) are not. In cases where a VASP relies on a third-party custodian, a blockchain wallet that initiated a certain VA transfer may not even be managed by the particular VASP. For this reason, simply returning the VA back to the 'from or originating address' identified by a blockchain explorer or scan may lead to the loss of the virtual asset. In the event that a VASP wishes to return the virtual assets back to the originator's account managed by the ordering VASP, it may need to separately collect the deposit address of the originator with the consent of both originator and intended beneficiary.



In case the originator is not the same person as the intended beneficiary, there is the complication of who to return the VA to: Is it back to the originator or to a wallet address in the name of the intended beneficiary managed by another VASP (among the approved VASPs that has completed the counterparty DD)?.

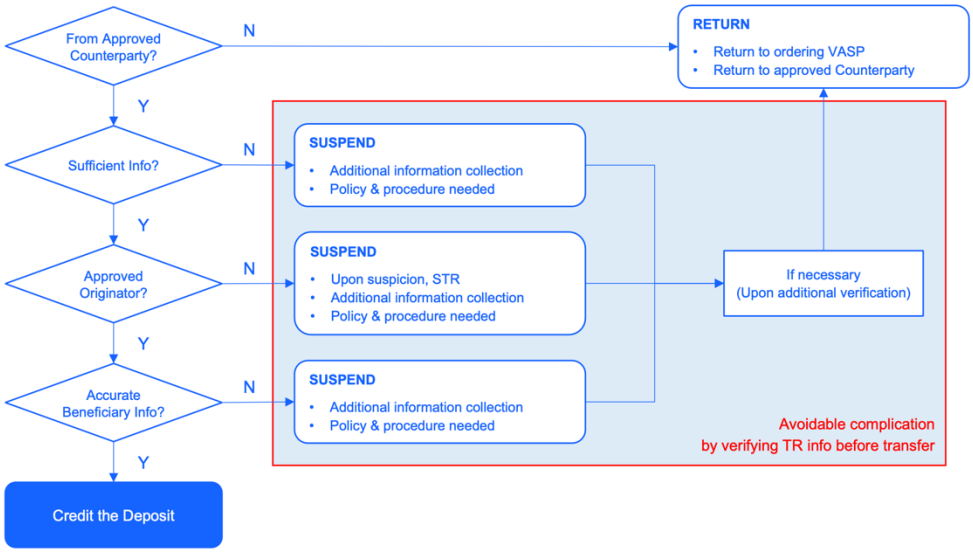
This is an interconnected problem with c) the applicability of Travel Rule to the return process. In the event that Travel Rule compliance needs to be applied to the return transaction, sending the transferred VA back to the originator may not be feasible since there is no guarantee that the originator (not a user of the VASP) has an

account among the approved VASPs. This is due to the unique characteristic of the virtual asset industry. Unlike the traditional financial industry, an ordering VASP can be anyone (e.g. unregulated VASP, illicit actor, private wallet, etc.) and can be outside of the approved counterparty list.

If it is possible not to apply Travel Rule to the return process, then returning the transfer back to the originator is a possible option. But even in this case, there needs to be specific consent from both the originator and the intended beneficiary regarding the collection of data and the return of assets. Name screening on the originator and on-chain screening on the requested destination wallet address (not 'from' address) will be necessary to avoid transferring assets to illicit actors. This transaction will generate a withdrawal transaction towards an 'out of approved VASP' and may need to pass sufficient internal approvals processes with written record.

Considering such complications, we are of the opinion that returning the VA back to the intended beneficiary's other account kept in an approved VASP (upon the consent of originator) via Travel Rule or an enhanced risk mitigation process is a more straightforward solution. Still, this practice runs the risk of abuse in the form of a chain of asset transfers, circumventing otherwise impossible transfers. For example, considering VASPs A, B, and C with counterparty relationships established only between VASP B and VASP C, the return policy can be abused to form a chain of transfer from VASP A then B then C, effectively allowing VASP A to indirectly transfer the assets to C. For this reason, the return can only be processed upon necessary considerations of relevant facts and internal approvals to discourage any abusive practice.

Lastly, if not mandated by a regulation, a VASP needs to make the decision whether to apply the Travel Rule or an enhanced risk mitigation measure upon returning the transaction. We are of the opinion that the Travel Rule or an enhanced risk mitigation measure should be applied even in the case of a Travel Rule return transaction. As described above, omitting Travel Rule does not make the return process any easier for a VASP or its user due to the responsibility of name screening and on-chain monitoring accompanied by data collection complications. Also, in case a user has a (Travel Rule not-compliant) deposit, the user usually has an account in another VASP, making the return more feasible. In case a VASP wishes to further mitigate the risk associated with a return transaction, limiting the beneficiary only to the first party (the user itself) could be a straightforward option as long as it can secure consent from the originator upon the intended return transaction.



All these complications described above can be significantly reduced by verifying the beneficiary prior to transferring VA.

Most importantly, as there is no guarantee that the beneficiary institution would conduct a proper alignment check on the received beneficiary information against the information they hold (due to delayed and varying levels of regulatory oversight in the VA industry), it is much safer for the ordering institution to verify beneficiary information prior to making the VA transfer. Otherwise, regulated institutions may end up transferring VA to illicit actors due to falsely declared beneficiary information, and the said institution may not even have the chance to detect it subsequently. For all these reasons, we strongly recommend that the ordering institution should verify the beneficiary prior to funds being transferred, at least in a VA context.

/* On a separate note, we have a minor concern on the interpretation of the footnote to para. 7(b). In the VA sector, we observe an increasing number of jurisdictions requiring the safeguarding of customer assets. For this purpose, the use of reliable third-party VA custodians is becoming a popular choice, and is even being mandated in some jurisdictions. In such cases, the funds (VA) of a customer may be stored in the safeguarding institution of an ordering institution under an institution-to-institution safeguarding arrangement.

Even if all or part of the customer's VA are stored in the blockchain wallet managed by a safeguarding institution under such arrangement, the customer's funds (VA) are located and held in the ordering institution contractually. The customer is the customer of the ordering institution and there will be an account number assigned to the customer. In this regard, the financial institution where the customer's fund (VA) is located, in the context of footnote 1, para 7(b) will be the ordering institution (the customer is a customer of this institution) rather than the safeguarding institution (the customer is not a customer of the safeguarding institution). This would be comparable to customer A putting their money in Bank A and subsequently, Bank A buying US T-Bill for treasury management purposes. In such scenario, customer A's funds are located in Bank A, not with the US government.

But depending on how various national regulators read the footnote in para. 7(b), there is a risk of recognizing the safeguarding institution as the financial institution holding the customer's funds, leading to a complication of the R.16 exercise for the ordering institution. We foresee this confusion stemming from misreading the draft revision. It is better to avoid it.

Q.16 - Do you agree with the proposed changes to the Glossary definitions?

Yes, we agree with the proposed changes to the Glossary definitions.

j. Timing of implementation of R.16/INR.16 revisions

Q.17 - Do stakeholders have any views on the timelines for implementation of the proposed revisions to R.16/INR.16? What should be the lead time for implementation of the proposed new requirements and why?

In the VA sector, the proposed revision could be implemented immediately as we (VerifyVASP) have already been processing R.16 information submission and verification in compliance with our proposed draft revision. Even if additional data fields are needed for some of our members, our technical architecture allows for the flexible addition of data fields and for its verification.

For the non-VA sector, we are not qualified to answer this question.

Q.18 - Are there any issues that should be addressed in the proposed amendments, or wider issues concerning payment transparency, which will require clarification through FATF Guidance?

This is not a closing comment, but rather a specific issue concerning payment transparency. Expanding the scope of payment message recipients may not guarantee effectiveness against abusers utilizing complex payment chains. Residual risk remains, despite best efforts by financial institutions to mitigate AML/CFT risks around payments of value transfers. Worse yet, depending on the design, such requirements in isolation may pave a dangerous path to financial exclusion and de-risking, reducing the remit of regulated financial services. This would result in the exact opposite outcome to the FATF's intentions.

We are currently waging a war against ML/TF and as in any war, at any point of history, better technology usually leads to higher chances of winning. We observe that most of the financial regulations are focused on obtaining, verifying and submitting data, without describing or mandating what technological capability should be secured to utilize the said data. The discussion around specific technology is not (and should not be) a monopoly reserved for abusers. Omitting technology from the discussion can lead to an abundance of data but a shortage of intelligence around the utility of the data. Without a superior level of intelligence, financial institutions may not make any meaningful foray in the battle against abusers armed with the most evolved technology.

In this regard, we urge the FATF and national regulators to actively explore and share best practices using technology to fight against ML/TF risks. Even if some are at the experimental stage (as any prototype weapon), support from financial institutions and the public sector would help to develop these possibilities into a reliable weapon systems in this arms race. No fresh path to more effective ML/TF risk mitigation will be found without new technology.