The Wolfsberg Group
c/o Basel Institute on Governance
Steinenring 60 | 4051 Basel, Switzerland

February 26, 2024

Mr Jose Manual Campa
Chairperson
Ms Carolin Gardner
Head of Unit (AML/CFT)
European Banking Authority
Tour Europlaza
20 Avenue André Prothin
CS 3015492927 Paris La Défense CEDEX
France

Dear Mr Campa, dear Ms Gardner:

RE: Public Consultation on Preventing the Abuse of Funds and Certain Crypto-assets Transfers for Money Laundering and Terrorist Financing Purposes under Regulation (EU) 2023/1113

The Wolfsberg Group (the "Group") welcomes the opportunity to provide comments on the Consultation Paper "Travel Rule Guidelines", published on 24 November 2023 (EBA/CP/2023/35). The Group believes that it would be beneficial to the industry to have greater clarity with respect to the obligations for institutions emanating from the underlying "Funds Transfer Regulation" (FTR) and has structured its feedback accordingly. The Travel Rule Guidelines present an opportunity to look at the requirements so as to facilitate impactful controls, proven to manage financial crime risk effectively.

While this is outside the scope of the current consultation, the Group recommends that the FTR itself be reviewed to ensure it addresses current payment market practices such as many-to-many payments[1], the use of virtual IBANs/equivalents, the use of non-Swift messaging and the inclusion of ISO 20022 terminology.

The Group's response focuses primarily on Payment Service Providers (PSPs) and fund transfers. It is organised into general comments first, followed by commentary on specific sections.

High-level Considerations

The Group considers that more explicit guidance from the EBA would be beneficial in the following areas:

Transfer of funds requirements

Role differentiation

- In a transfer chain, each PSP has a different role and, as a result, has access to different sets information. We believe that the responsibilities assigned to each actor – payer PSP, intermediary PSP (IPSP), payee PSP – need to reflect this. The draft Guidelines do not make this distinction and, in particular, fail to acknowledge the position of IPSPs, which lack the ability to collect or process information on non-customers.
- In many cases, e.g. Paragraphs 4, 21, 22, 26, 29 and 43, the requirements set out in the Guidelines should only be applicable to payer PSPs, as only they are in possession of the necessary information to satisfy the requirements.

[1] As the FTR only appears to envisage transfers of funds from a single payer to several payees.

- For a more detailed view of the Group's stance on roles and responsibilities in the transfer chain, please refer to the 2023 Wolfsberg Group Payment Transparency Standards.[2]

Treatment of batch[3] payments

- We are concerned that the requirements introduced in Guidelines 3.2 may be interpreted as a new obligation to "un-batch" all payments, with the information on underlying payers and payees to be passed on to the next PSP including to and by IPSPs.
- The Group suggests that the Guidelines provide an acceptance of the limitations institutions face in obtaining Due Diligence information on non-customers and recognition that consumers may be unwilling to provide information to an institution with which they have no relationship. The responsibility for complying with the FTR in the scenario of batch transfers should be clarified and placed on the payer rather than the intermediary PSP.

Information accompanying transfers of funds

- It is standard industry practice to provide, in a payment message, the payer's address *or* document number and account number *or* the date and place of birth. As opposed to what Guideline 4.3 suggests, the (offline) transmission of a combination of these data points should only be considered relevant or necessary where the payer is not sufficiently identified.

Detecting missing or incomplete information

- Certain provisions in the draft Guidelines appear to suggest that ex-post monitoring for missing or incomplete information – which is the expectation in the FTR – is not permitted (see paragraphs 33, 43, 44, 46, and 51).

Consistency in, and clarification of, terminology

In several instances, there would be benefit in clarifying the terminology used to ensure a consistent interpretation of requirements, thereby allowing for greater standardisation. Key examples include:

- The lack of definition of clear attributes that constitute "linked" transactions in Guideline 2.2.
- The lack of a specific definition of "messaging systems" in Guideline 3.1 including ambiguity in the use of the terms "payment and settlement" and "transfer and settlement" systems.
- The introduction of the new terms "unambiguous" and "inconsistent" in Guidelines 4.3 and 5.4 respectively.

CASP-focused remarks

- Although the Group's feedback is centred on PSPs and funds transfers, we request that the Guidelines address the fact that CASPs cannot block or reject transfers akin to what happens in fiat currencies (Guideline 7.1) and the impossibility of identifying self-hosted wallets (Guideline 5.3).
- We also suggest that the Guidelines clarify that transaction fees relating to crypto asset transfer are not within scope of the travel rule; the reasons for the exemption are outlined below under Guideline 2.

In the sections that follow, feedback is provided as to specific provisions in the proposed Guidelines.

Detailed Considerations

Guideline 2, Exclusion from the scope of Regulation (EU) 2023/1113 and derogations

We request that the EBA confirm that transaction fees (gas fees) are out of scope of the FTR and these Guidelines, given that the unique characteristics of paying transaction fees will preclude the ability to apply

[2] https://db.wolfsberg-group.org/assets/13422898-fba1-44b3-9679-a8c7406e9e78/Wolfsberg%20Group%20Payment%20Transparency%20Standards%202023.pdf

[3] "Batch" is used here for consistency with the FTR and these Guidelines to capture any aggregation of payments, sometimes referred to as "bundled" or "bulk" payments.

these requirements to certain distributed ledger technologies. This aligns with the exemption in the Financial Action Task Force (FATF) Guidance on Virtual Assets and VASPs (paragraph 180).

Guideline 2.1, on determining whether a card, instrument or device is used exclusively for the payment of goods or services as per Article 2(3) point (a) and (5) point (b) of Regulation (EU) 2023/1113

We note that Article 2(3) exempts transfers of funds executed using a payment card, electronic money instrument, mobile phone or other digital or IT prepaid or postpaid device from the Regulation provided that the card, instrument, or device is used *exclusively* to pay for goods and services. We encourage the EBA to focus its guidance on the functionality of cards, instruments and devices provided by PSPs to their customers (the payers) and not to requiring PSPs to monitor how those cards, instruments and devices are used by customers. Industry practice is to consider the functionality of the card, instrument or device provided to customers, exempting those that cannot be used to make fund transfers from the Regulation (such as closed loop store cards). It is impracticable to monitor usage of card, instrument or device that can be used both for payment of goods and services and funds transfers in order to determine which customers that own that card, instrument or device qualify for this exemption.

While the payer's PSP may reasonably be expected to know whether its customer (the payer) is engaged in economic or professional activity, the payer's PSP would not have this information available about the payee unless the payee is its customer. We recommend that the EBA state that the requirements are not mandatory but rather suggested guidelines for PSPs to consider in their assessment of whether the transaction initiated by their customer is used for the purchase of goods or services. Similar considerations are applicable to transfers of crypto assets and Paragraphs 5(b) and 5(c).

In addition, we believe that the industry and consumers would benefit from the clarification of what falls in the category of goods and services through some real-life examples. For instance, whether the purchase of FX currencies and an associated transfer of funds in another country would be considered a service.

Guideline 2.2, on Linked transfers in relation to the 1000 EUR threshold (Article 2(5)(c), Article 5(2), Article 6(2) and Article 7(3) of Regulation (EU) 2023/1113)

We encourage the EBA to reconsider its guidance that funds transfers should be treated as linked where "sent by the same payer to the same payee or persons linked with them" and "sent from [...] different payers to the same payee or persons connected with them" (**Paragraph 7(b)**). We agree that a reasonable threshold should be set for verification measures to avoid impairing the efficiency of payment systems and to balance the risk of driving transactions underground. However, it is neither practical nor reasonable for PSPs to identify payers or payees that are "linked", for example through family or professional connections, when they have only one of the parties as a customer. We caution that a new definition of "linked transfers" that incorporates 'persons connected' to the payer or payee sets an overly strict threshold that will result in PSPs being unable (and/or choosing not) to apply the EUR 1000 verification threshold. There is an additional risk that this may marginalise vulnerable people who may difficulty verifying their identity to the prescribed standard and could therefore ultimately drive transactions underground, away from regulated PSPs and out of sight of law enforcement.

In the same paragraph, a more specific definition of what is considered a "short timeframe" would enable PSPs to evaluate their ability to comply with this part of the Guidelines.

Guideline 3.1, on the interoperability of protocols

The term "messaging systems", as distinct from transfers, payments and settlement systems, is not defined in Article 3 of the FTR nor in the Glossary on page 13 of the Guidelines. For this reason, it is open to varied interpretation. As the Guidelines apply to Funds Transfers, we would recommend that the term "messaging systems" be defined solely in the context of transfers, payments and settlement systems that move both information and value.

Paragraph 11 fails to recognise practical challenges that arise from the use of different protocols or messaging systems, across different jurisdictions, where differing formats are used that have varying levels of capacity to include information. While the Group supports the premise aimed at maintaining data integrity, the language as drafted ("Where PSPs […] cannot ensure that their systems are able to convert information into a different format without error or omission, the PSPs […] should not use such systems") is not aligned to industry practice. We suggest amending the language as follows: "Where PSPs […] cannot <reasonably be expected to> ensure that their systems are able to convert information," acknowledging that PSPs/IPSPs/CASPs/ICASPs should have processes in place to avoid the truncation of relevant information (e.g. by using abbreviations) and prioritise the information to be transmitted to the next PSP in the transfer chain.

Guideline 3.2, on Multi-intermediation and cross-border transfers

The Group recognises that this Section aims to address the complexities of cross-border/domestic payment flows. Nonetheless, the proposed solution in **Paragraph 17** ("Where the transfer is made from a cross-border channel to a domestic channel the domestic IPSPs or PSPs should assess whether the transfer is correctly identified as a cross-border transfer.") may be viewed as a new requirement which goes beyond the scope of the FTR and presents significant implementation challenges. The absence of an internationally applied cross-border transfer indicator/marker in payments and messaging systems, as well as the technical limitations of some Swift and non-Swift messaging systems in allowing the transmission of all relevant information to the next PSP, will make it challenging – if at all possible – for PSPs to be able to comply with the Guideline as it is currently drafted.

The Group recommends revising the language to "PSPs should select the domestic system that maximises the transparency of the cross-border nature of the payment and the information about the parties to the payment transmitted to the next PSP in the payment chain, that can be readily understood by all intermediary and/or beneficiary PSPs." This retains the spirit of maximising payment transparency. For further context, please refer to the Wolfsberg Payment Transparency Standards.

In addition, **Paragraph 17** ("…when the PSP or IPSP handling a transfer does not have a direct relationship with the payer, that PSP or IPSP should ensure that the next PSP in the transfer chain receive the information on the payer and payee.") may also have significant unintended consequences with regards to batch transfers. The indication that PSPs/IPSPs should ensure that the next PSP in the transfer chain receives the information on payer and payee can be construed as a requirement to un-batch all batch payments, and for the information on underlying payers and payees to be passed on to the next PSP. If interpreted this way, this requirement will have a considerable impact on how the industry operates, as illustrated in our comments in the section below (Guideline 3.3). The Group is firmly of the view, as set out in our Payment Transparency Standards, that IPSPs should pass on all the information that they receive within payment messages, to the fullest extent permitted by the relevant payment and messaging systems, to the next PSP in the transfer chain. Provided that adequate steps are taken to ensure complete message transmission, the Guidelines should state explicitly that further requirements to un-batch will not apply.

We recommend that **Paragraph 17** be revised so that it is clear that it refers only to transfers that have not been batched, and that our comments relating to that Paragraph also be considered for **Paragraph 19**.

Guideline 3.3, Batch transfers (Article 6(1), Article 7(2) (c), Article 15, Article 16(1), Article 20 of Regulation (EU) 2023/1113)

With regards to batch transfers – **Paragraph 19**, we would reiterate our previous comments (see Paragraph 17) that the primary responsibility for ensuring compliance with the FTR should be that of the payer PSP (or payee PSP for direct debit transactions), as it is best placed to capture, verify, and retain the required information given that it maintains the customer relationship. If an IPSP were required to receive all the underlying information then the benefits of batching will be negated as, rather than processing a single payment (without underlying information), the IPSP will effectively be processing all the underlying

payments along with their respective information, which will inevitably have an impact on both costs and speed of execution.

The increase in costs to consumers would be due to a loss of the economies achieved by batching and the impact on the speed of execution of the transfer would be a result of the additional controls that will need to be performed. These include:

- If existing batch payments were required to be un-batched, then controls currently applied to a single payment (without payer and payee information) would have to be applied to each individual payment in the batch, thereby increasing the likelihood of false positives from screening which would increase costs and possibly introduce delays in the execution of the payments.
- If "missing information" is routed "via an alternate channel mechanism", the PSP will need to reconcile the two different transmissions of information, possibly sent at different times, so that screening of the information on the parties to, and purpose of, the payment is performed prior to the payment being processed which may cause delays. Transaction monitoring systems would also need to be reconfigured to be able to receive data from two different sources.

Guideline 4, on identifying the specific data points to be transmitted as part of the information required under Article 4(1) and (2) and Article 14(1) and (2) of Regulation (EU) 2023/1113
The Group suggests that the EBA focus on the following challenges with respect to **Section 4.3**.

To foster more standardisation, and leave less room for interpretation of what these terms mean, we suggest that **Paragraphs 23(a)** and **23(b)** should be consistent with the proposed text for the so-called EU AML/CTF Regulation (COM/2021/420 final) and particularly Article 18(1). As such, in 23(a), we recommend that "habitual residence" be changed into "usual place of residence," and that the word "postal" be inserted before "address" in the sentence "the PSP or the CASP may use an address…". In paragraph 23(b), we recommend changing "registered office" into "address of the registered or official office, or, if different, the principal place of business".

We strongly suggest that Post Office Box numbers be considered as an acceptable identifier of address for jurisdictions where these are considered acceptable and adequate absent any other form of address, (**Paragraph 25**), given that these are considered as acceptable in a number of jurisdictions. As in prior comments, only the PSP holding the customer relationship will be able to know if an address is "virtual".

We encourage the EBA to reconsider its guidance in **Paragraph 26**. Firstly, it is not industry practice for PSPs to include the payer's official personal document number, customer number or date and place of birth in outbound payments. Official personal document number and date and place of birth are interpreted as alternatives to providing the payer's address. A customer identification number will typically only be provided when the payer does not have an account. As such, industry practice is typically to provide payer's name, account number (or customer identification number where there is no account), address (including the country) and date and place of birth (the latter when needed). This information is sufficient for sanctions screening, analysis of suspicious activity and for assisting law enforcement in detection, investigation, and asset recovery.

We welcome acknowledgement in Regulation (EU) 2023/1113 that Union action should take account of developments at an international level. We note that peer countries such as the UK and US, do not require payments to contain all the data points set out in paragraph 26. As such, if EU PSPs are required to monitor and suspend/reject payments that do not include all this information, the result will be disruption of legitimate payments into the EU to the detriment of the soundness of the financial system and of EU consumers and businesses and place EU PSPs at a competitive disadvantage.

The introduction of the term "unambiguous" in **Paragraph 26**, without further clarification, will present significant challenges to the speed of payment processing and resultant delays for consumers and businesses. As the FTR does not use such terminology, referring only to "accurate" and "complete"

information, this appears to introduce a higher standard than outlined in the FTR. We recommend strongly that the term be removed, as its subjective nature may inadvertently create the very ambiguity that the Guidelines are seeking to resolve, and the language used in the FTR ("complete" and "accurate") retained with the possibility to further clarify these requirements by referencing the Basel Committee on Banking Supervision's language on "manifestly meaningless information"[4]. Should the EBA nonetheless retain the term, it would need to be clearly articulated how this would substantiate the regulatory requirements it is linked to, as well as what would qualify as "unambiguous."

Guideline 4.4, Providing an equivalent Identifier to the LEI of the payer (Article 4(1) point (d) of Regulation (EU) 2023/1113), of the payee (Article 4(2) point (c) of Regulation (EU) 2023/1113), of the originator (Article 14(1) point (e) of Regulation (EU) 2023/1113) and of the beneficiary (Article 14(2) point (d) of Regulation (EU) 2023/1113)

The Group requests clarification as to whether all the criteria listed are required or whether the items can be taken as a list of alternatives.

Guideline 5.3, Monitoring of transfers (Articles 7(2), Article 11(2), Article 16(1) and Article 20 of Regulation (EU) 2023/1113)

We strongly recommend that the EBA amend **Paragraph 33** ("…procedures how to determine which transfers are appropriate to be monitored *before* the transfer takes place and which transfers are appropriate to be monitored *during* the transfer") to acknowledge the possibility of deploying ex-post monitoring for detecting missing information. This is clearly allowed under Article 7(2) of the FTR ("…including, where appropriate, monitoring *after* or *during* the transfers") and called out in Paragraph 29(b) of these Guidelines ("a combination of monitoring practices *during* and *after* the transfer…").

With respect to the list of risk factors set out in **Paragraph 34**, we believe it is far more effective to assess a combination of risk relevant factors, rather than imply or require that all of them be considered; we therefore suggest that the language be rephrased, as follows: "PSPs, IPSPs, CASPs and ICASPS should consider one or more among the factors below:".

On CASPs specifically, in relation to **Paragraph 34(e)**, we wish to bring the EBA's attention to the fact that, at present, it is not possible to fully identify and differentiate a hosted or self-hosted wallet.

Guideline 5.4, Missing information checks (Article 7 (2), Article 11 (2), Article 16 (1) and Article 20 of Regulation (EU) 2023/1113)

Referring to the earlier point, the Group suggests that the EBA update **Paragraph 37** to focus only on empty mandatory fields as defined by regulation and provide clear guidance on how to determine whether some information is "inconsistent"; if no such guidance is possible then we recommend deletion of the term. As set out in this response, the industry is familiar with the concepts of missing, incomplete, inaccurate information. The introduction of new terminology without sufficient clarification would contribute to hinder consistency in the application of requirements.

Guideline 6.2, Rejecting or returning a transfer (Article 8(1) point (a), Article 12 point (a), Article 17(1) point (a) and Article 21(1) point (a) of Regulation (EU) 2023/1113)

Requests for Information (RFIs) turnaround times can be affected by e.g. the number of parties in a payment flow, language differences between those parties, time zone differences and the presence of non-working days. Placing limitations on the turnaround times for RFIs may therefore not be practicable and we suggest that some assurance that longer than three or five working days (though still reasonable) timelines can be applied as this would be beneficial to the effectiveness and desired intent of the process and not cause suspended payments to be returned simply because the indicative RFI turnaround time has been exceeded rather than for risk-relevant reasons.

[4] Due diligence and transparency regarding cover payment messages related to cross-border wire transfers (https://www.bis.org/publ/bcbs154.pdf).

Moreover, while the Group recognises the importance of the content of this section, we note that many CASPs will not have the ability to reject payments, which should be accounted for in the Guidelines.

Guideline 6.3, Requesting required information (Article 8(1) point (b), Article 12(1) point (b), Article 17(1) point (b) and Article 21(1) point (b) of Regulation (EU) 2023/1113)

The Group is concerned that, as currently phrased, **Paragraphs 43 and 44** do not leave room for ex-post monitoring. Articles 8(1)(b) and 12(1)(b) of the FTR state explicitly that, when information is missing or incomplete, PSPs may, on a risk-sensitive basis, "request the required information on the payer and the payee before or after crediting the payee's payment account or making the funds available to the payee/the transmission of the transfer of funds". Paragraph 43 of the Guidelines sets out a 3- or 5-working day deadline for obtaining the required information and Paragraph 44 states that, if an RFI is sent, the prior PSP/IPSP in the transfer chain needs to be notified that "the transfer has been suspended due to missing or incomplete information". This suggests that the transfer is necessarily suspended before processing and does not recognise the possibility of ex-post monitoring and review. Equally, **Paragraph 46** requires PSPs/IPSPs to either reject or execute the transfer if no response is received by the set deadline, which assumes that the transfer is still suspended. Indeed, it is not possible to reject or execute a transfer that has already been processed. The EBA should address the inconsistency between the requirements of SEPA Instant Payments where payments must be made or rejected within specified timeframes and the suspension option set out in these Guidelines.

In addition, under **Paragraph 43**, it is unclear whether the responsibility lies on the PSP's customer to supply the missing/incomplete information within the timeframe and if it is not met, who should be held accountable.

Guideline 6.4, Executing a transfer (Article 8(1), Article 12, Article 17(1) and Article 21 of Regulation (EU) 2023/1113)

We welcome the acknowledgement in **Paragraph 51** that PSPs may detect missing/incomplete information or inadmissible characters, ex post. However, as highlighted in our comments to Paragraphs 33, 43, 44 and 46, the Guidelines should also recognise that the receiving PSP can pass the information along to the next institution as received and take remedial actions regarding missing/incomplete information ex post. Ex-post monitoring can identify data completeness issues without impacting the timeliness of payment processing (and hence minimising inconvenience to the payer/payee) and can be used to identify remedial action needed to be taken by the PSPs involved. This is in line with existing Repeatedly Failing FI requirements in the FTR.

Guideline 7, Repeatedly failing PSPs, CAPSs, IPSP or ICASPs (Article 8 (2), Article 12 (2), Article 17 (2), and Article 21 of Regulation (EU) 2023/1113)

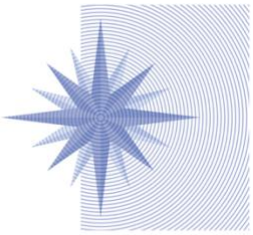
The Group stresses that it will be both inefficient and ineffective to leave individual PSPs and CASPs to determine the criteria as to when entities should be considered as "repeatedly failing" and if so, what action should be taken. This could promote an inconsistent approach which prevent establishment of a level playing field. We recommend that standardisation be undertaken via a Regulatory Technical Standard, which should set out both the criteria for categorising institutions as "repeatedly failing" institutions and actions for remediation. This should also include possible restrictions in extreme cases where requests for remedial actions sent from PSPs/CASPs do not result in changes in behaviour by the entity deemed as 'repeatedly failing'.

Paragraph 59 should address the fact that CASPs do not have the possibility to block or reject funds received via distributed ledger technologies.

Thank you in advance for your consideration of our feedback. Please do not hesitate to contact the Wolfsberg Group Secretariat at info@wolfsberg-group.org if you have any questions or would like to discuss this submission further.

Yours sincerely,

Alan Ketley
Executive Secretary
The Wolfsberg Group



Banco Santander
Bank of America
Barclays
Citigroup
Deutsche Bank
Goldman Sachs
HSBC
JPMorgan Chase
MUFG Bank
Société Générale
Standard Chartered Bank
UBS

the Wolfsberg Group

Wolfsberg Group Payment Transparency Standards

Introduction

The Wolfsberg Group (the Group) has always viewed payment transparency as a foundational element to an effective financial crime compliance programme. This began with the Group's support for the Financial Action Task Force's (FATF's) Special Recommendations (specifically Special Recommendation VII on wire transfers), in its 2002 Statement on the Suppression of the Financing of Terrorism and developed further in the Group's 2007 Statement on Payment Message Standards (made jointly with The Clearing House Association). The Group then provided significant institutional support to SWIFT (and partnering competent authorities) in embedding the MT202COV, and most recently published Payment Transparency Standards, which included strong advocacy for ISO 20022 in 2017.[1]

Since 2017, innovation has advanced in payment services and open banking, pushing the international financial system to be more efficient, competitive, and inclusive. However, the associated operational and financial crime risks have not necessarily always been quantified. These revised Standards highlight those risks in the context of payment transparency and – in the absence of globally uniform standards and guidelines, which continue to vary across jurisdictions – detail a responsible way forward for all stakeholders involved in payments.

Today, where one actor's position in ensuring payment transparency starts and ends is no longer as clear-cut as when electronic payments were almost entirely initiated via a regulated bank and moved mainly through SWIFT messages. It is now necessary to address the roles and responsibilities of all actors in a payment chain, including nested parties, via various payment communication channels, irrespective of the nature of the stakeholders involved and whether or not they are banks. Legacy payment infrastructure handles increasing volumes of data, and understanding by all stakeholders (including supervisors) needs to improve on how new actors, pursuing unique payment models, challenge payment transparency requirements. Terminology

[1] ISO 20022 is an ISO standard for electronic data interchange between FIs that includes payment transactions, securities trading and settlement information, credit and debit card transactions and other financial information. Throughout this document, ISO 20022 terminology is used to refer to payment parties. More information can be found here: https://www.iso20022.org/faq.page.

is also changing as payment messages are increasingly formatted according to the more structured ISO 20022 framework.

As a result of these developments, and in alignment with the work done on effectiveness in recent years[2], the Group has taken the decision to replace the 2017 Payment Transparency Standards to reflect the evolution in payment methods, infrastructure, and landscape. Specifically, while building on the 2017 document and maintaining the same basic criteria and definitions of formatting payment message information, these revised Standards:

- Employ terminology that can be applied broadly across the financial services industry, including new market entrants who may or may not be regulated to the same degree as traditional banks. As such, Financial Institutions (FIs) are referred to as "payment service providers" (PSPs)[3]. Moreover, in line with ISO 20022 lexicon, the ordering FI or payer PSP is defined as the "debtor agent PSP", the intermediary FI as the "intermediary agent PSP"[4], and the beneficiary FI or payee PSP as the "creditor agent PSP" – agnostic to whether the underlying entity or "agent" is a bank or non-bank FI (NBFI). The revised Standards also begin to identify how various capabilities within the ISO 20022 structure can be utilised to enhance payment transparency, though it is recognised that such advances will only become widespread as adoption of, and adherence to, ISO 20022 standards increases.
- Expand the list of key stakeholders previously addressed by the Standards to include payment market infrastructures (PMIs) and their competent authorities[5], recommending specific areas where clearer guidance from these actors would result in better harmonisation in the application of payment transparency standards across PSPs;
- Re-establish the core principle, despite various new and emerging payment methods, that a payment is a payment, and as such the debtor agent (the ordering FI) – bank or non-bank – maintains the obligation to ensure that a new payment is structured appropriately, identifying clearly the debtor and creditor in any transfer of funds;
- Clarify the roles and responsibilities of the intermediary agent (the intermediary FI) and the creditor agent (the beneficiary FI), including their limited ability to identify suspicious activity and/or conduct sanctions screening when the information accompanying a payment is limited; and
- Assist the industry and associated stakeholders, through payment flow diagrams (see Appendix A) identifying payment transparency challenges, including in payments with high levels of intermediation. This includes, for example, instances where several individual payments are bundled into a single message instruction (especially in a cross-

[2] See The Wolfsberg Group – Statement on Effectiveness (2019), Developing an Effective AML/CTF Programme (2020), Demonstrating Effectiveness (2021), Effectiveness through Collaboration (2022).

[3] In this document, PSP is used to capture the full spectrum of payment service institutions that provide fund transfers, to include credit transfers, direct debit, money remittances whether domestic or cross-border, and transfers carried out using a payment card, an electronic money instrument, mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics. This includes traditional banks and money service businesses (MSBs) as well as entities commonly referred to as third party payment processors and electronic money institutions, among other PSP types.

[4] For the purpose of this paper, we have defined intermediary agent PSPs as the intermediary FI(s) in a payment chain other than the debtor agent PSP and creditor agent PSP.

[5] The term 'competent authorities' is used as defined in the glossary of the FATF Recommendations and refers to "all public authorities with designated responsibilities for combatting money laundering and/or terrorist financing".

border context),[6] payments associated with "goods and services", and situations where a payment that may appear to be domestic in nature is actually a cross-border payment.

The Standards

These Payment Standards should apply to:

- Cross-border payments[7]
- Domestic payments[8], as applicable under local regulations, including domestic PMIs
- All fiat currencies, including digital representations of fiat currencies such as Central Bank Digital Currencies (CBDCs)[9]
- Payments regardless of value, including transactions carried out using a credit, debit or prepaid card where the underlying intent of the transaction is to effect a person-to-person transfer of funds
- Debtor, intermediary, and creditor agent PSPs.

While these Standards recognise instances where local regulation establishes practical exceptions or exemptions to traditional payment transparency requirements (e.g. transactions carried out using credit, debit, or prepaid cards for the purchase of goods or services), the Standards highlight the risk of misuse of these provisions and propose additional guidance on the roles and responsibilities for interpreting the correct application of such exclusions. The Standards also recognise that in some jurisdictions, collection agent models are permitted whereby the PSP may be considered the legal debtor or creditor of a payment, operating on its own behalf, and reflected as such in the payment message.

These Standards will be of use to parties working on the introduction of new payment methods and platforms, payments, and compliance specialists, and to parties drafting regulation and regulatory guidance to address information requirements on funds transfers. The Standards are not intended to apply directly to digital assets but should be of value for digital asset service providers committed to the basic principles of payment transparency, as well as those involved in the development of digital assets, including in the design of CBDCs. As the payments landscape and supporting technologies continue to develop, the capability to uphold these Standards will further support enhancements in payment transparency.

The sections that follow address the applicability, roles, and responsibilities of the Standards across key stakeholders within the payment chain: (1) the PMI(s) and the competent authority(ies); (2) all PSPs, irrespective of their role in the payment chain; (3) debtor agent PSPs; (4) intermediary agent PSPs; and (5) creditor agent PSPs.

1. The PMI(s) and the competent authority(ies)

Clarity is required for PSPs on the permissible activity that may pass through a PMI, and the underlying roles and responsibilities of the debtor, intermediary, and creditor agent PSPs in

[6] "Bundled" is used here generically to capture any form of aggregation of payments, sometimes referred to as "batch" or "bulk" payments. Specific bundling typologies and the associated risks are addressed over the course of these Standards. "Cross-border" describes transactions where the debtor agent PSP, intermediary agent PSP or creditor agent PSP are in different jurisdictions.

[7] As may be defined under local regulations.

[8] As may be defined under local regulations.

[9] A CBDC is a digital asset for payments or a digital form of money issued by a central bank, denominated in the national unit of account, for wholesale or retail use, and representing a direct liability of a central bank in a single fiat sovereign currency. CBDCs are distinct from virtual currencies as they are legal tender and backed by a Central Bank/Government authority. CBDCs may or may not be on a distributed ledger technology.

channelling and receiving funds through the PMI. Given that PMIs often use different payment message formats, the PMI rulebook should specifically address, in a consistent way, the degree to which the PMI permits intermediated payments and how such payments (including the payment parties) should be captured according to the PMI's message format. The PMI rulebook should also clearly state the compliance obligations of the debtor, intermediary and creditor agent PSPs in their relationship with the PMI.

The rule-setting body of the PMI should consider:

- Ensuring that the specific financial crime compliance and payment transparency roles and responsibilities of all participants associated with the PMI (e.g. direct participants, indirect participants, agents, sponsored participants, "reachable BIC" participants and similar roles), as well as associated due diligence requirements, if any, are defined. This should include all PSPs that, while not registered formally with the PMI, leverage correspondent relationships with PMI participants to settle payments via the PMI.
- Establishing the levels of intermediation permitted by PMI participants and how various levels of intermediation are to be captured in the payment message format(s) supported by the PMI. Guidance should also explicitly address, if applicable, cases where permitted levels of intermediation in the PMI exceed available field or character space in a payment message format to capture all intermediary agent PSPs. Guidance on formatting should also include instances where the payment started in a different PMI, if permitted.
- Determining what types of payments are permitted to be cleared via the PMI and the corresponding formatting guidance/requirements. This may include, but not be limited to, a provision for PSPs to indicate if a payment is cross-border (including where PSPs use a combination of internal net settlement cross-border payments and domestic PMIs to facilitate payment offerings to customers), bundled payments (particularly those that are cross-border), use of structured data to improve data quality (thus also improving transparency objectives and transaction monitoring/screening outcomes), and payments associated with the purchase of "goods or services" where distinct approaches to payment transparency may be permitted, e.g. for goods and services purchased via credit cards.
- Identifying appropriate technological enhancements to facilitate evolving payments and settlements adequately. This may include enhancements to payments and/or messaging systems to add fields or character space to capture intermediary agent PSPs and additional message information related to cross-border payments, bundled payments, or payments associated with the purchase of goods or services via a credit, debit, or prepaid card, or to include indicators for domestic payments that originated cross-border. These technological enhancements are indispensable for PSPs to be able to uphold many of the Standards included in this document.

The competent authority should be responsible for:

- Providing guidance on the circumstances under which bundled payments are permitted (if allowed by host country regulation) and those in which a PSP is only processing final settlement/disbursement of transactions. Special attention should be placed in distinguishing among the various forms of bundling: from "one-to-many" (e.g. salary disbursements) or "many-to-one" (e.g. merchant servicing), where the risks are less significant, to "many-to-many" (e.g. remittances from various debtors/originators bundled into a single payment that is then unbundled at its destination to pay several

creditors/beneficiaries). The latter leads to less transparency for intermediary agent PSPs and increased risk, particularly with cross-border payments.

- Clarifying applicable requirements for PSPs when using alternatives to payment account numbers (where permitted by the host country), for example virtual receivable account numbers or tokenised account numbers.
- Providing clarity on the criteria that a debtor agent PSP must apply in determining if a credit, debit, or prepaid card, digital wallet, electronic money instrument or similar payment device or instrument is used for effecting a purchase of goods or services as opposed to a person-to-person transfer of funds; and the distinction between a transaction aimed at "topping up" or increasing an available balance on a payment application or wallet (normally a domestic transaction) versus the instruction of those funds by the debtor to the creditor in a person-to-person transfer (especially when cross-border).
- Determining the circumstances under which a PSP is permitted to consider itself the debtor or creditor, e.g. when using a collection agent model and thus conducting activity on its own behalf.
- Clarifying the Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) and sanctions compliance expectations of an intermediary agent PSP in the PMI given, for example, "by, at, or through" reporting requirements in some jurisdictions, while recognising the challenges an intermediary agent PSP faces in monitoring the compliance of the debtor agent or other intermediary agent PSPs in their interpretation and application of payment transparency requirements.

It is critical that the competent authority recognises in guidance, in their supervisory activity, and in enforcement how methods that limit transparency in a payment – which are permitted by regulation – impact the effectiveness of intermediary and creditor agent PSP controls on monitoring for suspicious activity and enforcing sanctions compliance. Such an understanding should be reflected in rules promulgated by the authority (or appropriate body) and through the authority's supervisory examinations. For example, intermediary agent PSPs can only be expected to conduct real time sanctions screening on the information that is included in the message. The intermediary agent PSPs should not be held responsible, for instance, in enforcing sanctions compliance for multiple underlying debtors or creditors in a "many-to-many" bundled payment scenario where debtor or creditor information is not provided (as illustrated in more detail in Section 3).

2. All PSPs, irrespective of their role in the payment chain

The payment message standards to be observed by all PSPs are as follows:

- PSPs should not omit, delete, or alter debtor or creditor information in payment messages or orders for the purpose of avoiding detection of that information by any other PSPs in the payment process; changes should be based solely on correcting errors or enhancing message details to facilitate settlement and increase transparency.
- PSPs should accurately reflect the roles of all participating parties and agents in appropriate fields to the fullest extent permitted by the PMI, pending the technological enhancements to be implemented by PMIs as referenced above (e.g. in transitioning to ISO 20022). Payment information should be readily understandable by parties in the payment chain, in accordance with applicable laws and regulations, the PMI's rulebook, and the associated message format, such that the next PSP in the payment chain can

monitor and screen all parties effectively, even in circumstances of high payment intermediation.

- Subject to all applicable laws, PSPs should cooperate as fully as practicable with other PSPs in the payment process when requested to provide information about the parties involved and the nature of the transaction, including under legally permissible information sharing arrangements.
- For products which facilitate faster cross-border payments (e.g. through the combination of domestic PMIs and cross-border transfers), PSPs should select the domestic PMI(s) that maximise the transparency of the cross-border nature of the payment and the information about the parties to the payment transmitted to the next PSP in the payment chain, in a way that can be readily understood by all intermediary and/or creditor agent PSPs.
- PSPs should ensure that products and services provided to their FI and non-FI customers meet the PSP's own payment transparency requirements.
- PSPs should adopt payment transparency requirements consistent with these Standards and strongly encourage compliance with these requirements through their relationships with other PSPs.
- PSPs should move to adopt and use more structured and detailed payment formats at the earliest opportunity (e.g. ISO 20022), to improve data quality and thus also improve transparency objectives and transaction monitoring/screening outcomes.

3. Debtor agent PSPs – ordering institutions/payer PSPs

The debtor agent PSP is responsible for:

- Identifying, verifying, and conducting customer due diligence (CDD) on its customers (including any non-customer user of the PSP's origination services, e.g. as an occasional transaction or walk-in customer), as well as related record keeping in line with all regulations applicable to the PSP.
- Ensuring that messages contain all required information in compliance with FATF Recommendation 16, or as stipulated by applicable local regulations and guidance.
- Determining, based on the information provided by the debtor in the payment message, if the payments represent potentially suspicious activity or violate applicable sanctions programmes.
- Maintaining adequate records that permit the reconstruction of messages as required by local regulations.
- Implementing reasonable controls to determine if the intent of the payment is domestic or cross-border, indicating that intent clearly in the message where appropriate message tags/fields are available and to the fullest extent permitted by the relevant PMI, and providing all required information in the message as required by applicable laws, regulations, and guidance.
- To the fullest extent permitted by the relevant PMI, using the fields available in the payment message according to their intended purpose, so as to facilitate identification and understanding of payment information by all PSPs in the payment process, including:
    - Where permitted by the PMI and when available, using Legal Entity Identifier (LEI) or Bank Identifier Code (BIC) or equivalent reference codes to enhance the accuracy of identification information on relevant parties.

- Using the correct payment message for the type of payment and maximizing available capabilities (e.g. use of category purpose codes under ISO 20022), in line with relevant PMI guidance.
- Applying the appropriate criteria, as determined by the competent authority and associated PMI rulebook, on bundling (i.e. opting to bundle a series of payments into a single payment under a "one-to-many", "many-to-one", or "many-to-many" scenario), in accordance with the PSP's business model.
- Adopting applicable regulatory exceptions or exemptions that permit distinct types of information in a payment due to the payment's status as a purchase of a "good or service" (e.g. goods and services purchased via credit cards).
- When applying a collection agent model whereby the debtor or creditor agent PSP considers the funds "their own", and thus plays the role of the actual debtor or creditor, respectively.
- When initiating what will ultimately be a cross-border payment using domestic PMIs.

To ensure technical formatting requirements are met, the debtor agent PSP should, as the ordering institution:

A. Include **Name, Address** and **Account number** of the debtor, who is the originator of the payment, as the preferred approach to comply with local laws and regulations, which generally align to FATF Recommendation 16 guidance**.** In the absence of an account number, a unique transaction reference (UTR) number or similar code must be included. UTR numbers should only be used **in the case of a transfer not made from or to a payment account** – account numbers (or a similar static number associated with the debtor) are expected for all payments where there is a payment account established by the debtor agent PSP for its customer, the debtor.

   'Name' refers to the name of the customer ordering the payment (the debtor) as verified by the debtor agent PSP. The PSP should set out in its relevant policies and procedures which names are to be recorded in its systems and which of those names should be used for payments. These policies must be in line with all the regulations applicable to the PSP. For natural person customers, the name recorded in the PSP's systems should be the full name of the customer that was verified as part of CDD. For accounts held in joint names, the PSP should set out in its policy which names are to be recorded on its systems and which of those names should be used for payments. For legal entity customers (e.g. companies, partnerships), multiple names may exist such as registered legal name, trading name, "doing business as" name or commonly abbreviated name. The PSP should place preference on the registered legal entity name verified as part of CDD. For example:

	Registered Legal Name	**Trade Name/Doing Business As (DBA)**
Name	Eastern Finmark Corporation	Finmark or EFC
Purpose	The name given in the partnership agreement, articles of incorporation or other documents. It is used when communicating with the government or other businesses, e.g. when filing tax returns or buying property.	The name a business uses for advertising and sales purposes that is different from its legal name. A trade name can also be referred to as a DBA.

   'Address' refers to an address of the customer (the debtor) as verified or identified during CDD in accordance with the applicable laws and regulations by the debtor agent

PSP. Address information should be sufficient to identify clearly the location of the party/parties for sanctions screening and AML/CTF monitoring. It should include country and other aspects of address in accordance with the resident country conventions such as city, state/province/municipality, street name, building number and building name, and postal code. Having only a post office (P.O.) box as an address should be avoided except where no alternative exists due to market practices/limitations and is supported by local regulations. Address should be fully structured, when possible, and at a minimum employ a hybrid structure (structured town and country name, but potentially unstructured for street name, building number, etc. due to local naming conventions).

When not governed via structured formatting in the payment message, using full country names as recognised by the United Nations[10] will improve clarity. ISO 3166 2-character country codes[11] may be used as a preferred approach for PACS008, PACS009 and PACS009COV, Swift MT103, MT202 and MT202COV and related structured messages for debtor/originator and creditor/beneficiary fields as an alternative to full country name. Multiple addresses may exist, e.g. registered address, place of business address, mailing address. For example:

	Registered Address	**Place of Business Address**
Name	Eastern Finmark Corporation	Eastern Finmark Angola Branch
Address	17 Lords Avenue, London, United Kingdom, AC2V 5DV	Rua Cirilo da Conceo silva No.5, andar. Postal 1111. Luanda Angola
Purpose	A registered office is the official address of an incorporated company, association, or any other legal entity. Generally, it will form part of the public record and is required in most countries where the registered organisation or legal entity is incorporated.	A business address is the place where the real activity of the company is carried out, i.e. where the operations of the company are planned, controlled, managed, and executed.

The PSP should use the address verified as part of CDD. It is recognised that value may be found in utilising the "most relevant" address. The PSP should set out in its policies and procedures which addresses are to be recorded in its systems, and which are to be verified and used for payments (recognising that if an address is deemed to be "more relevant" than another, that address should be verified given its heightened relevance). This includes managing situations where multiple account holders with different addresses may exist, in which case the address of the primary or first named account holder is likely to be sufficient.

These policies must be in line with all the regulations applicable to the debtor agent PSP, as well as, when applicable under a correspondent relationship, the requirements established by the intermediary agent PSP that will facilitate the settlement of the payment for the debtor agent PSP's benefit.

Policies may also set out where a unique identifier code such as a BIC[12] or LEI is sufficient to identify the debtor where the debtor is an entity that can be identified appropriately without full name and address information.[13]

[10] See UN Member States list.
[11] ISO 3166 Country Codes.
[12] In certain instances, the same BIC may be shared among multiple entities.
[13] In developing their policies on usage of identifiers rather than names, FIs should consider industry publications such as the Payment Market Practices Group Global adoption of the LEI in ISO 20022 Payment Messages 2021.

B. Include **Name, Address,** and **Account number** of the creditor (the beneficiary or the payee), and ultimate creditor if applicable, to the fullest extent permitted by the relevant PMI. In the absence of an account number, a unique transaction reference number or similar code must be included. The inclusion of the address is strongly encouraged, represents best practice, and will facilitate faster processing, improve transaction monitoring quality, and reduce unnecessary requests for information (RFIs).

'Name' refers to the name of the creditor (the beneficiary) as provided by the originator of the transaction (the debtor). The name will not be subject to verification and the PSP should pass on the name as supplied by its customer.

'Address' refers to the address of the creditor as provided by the debtor (originator) of the payment transaction. Where possible, it should include country, state/province/municipality, city, street name, building number or building name and postal code in accordance with the resident country conventions. Having only a P.O. box as an address should be avoided except where no alternative exists. Creditor address should be passed on to the next PSP in the payment chain as supplied by the debtor and will not be subject to verification by the debtor agent PSP.

The debtor agent PSP should set out in its policy which creditor name(s) and address(es) should be requested from its customers (the debtor) for use in payment messages. These policies must be in line with the regulation of the applicable jurisdiction(s) of the PSP as well as the requirements established by the correspondent intermediary agent PSP, when applicable, that will facilitate the settlement of the payment for the debtor agent PSP's benefit.

C. **Implement controls to address "on behalf of" (OBO) payments.** An OBO payment is when the debtor agent's customer is making payments on behalf of an "ultimate originator" or "ultimate debtor". There are primarily two types of OBO payments: those made for the underlying customers of traditional corporate entities, e.g. multinationals with various subsidiaries with a centralised treasury department employing a payment factory function, and those made for businesses representing third parties, e.g. law firms. Such situations should be managed by the debtor agent PSP with regards to the CDD requirements as stated below, and identified by using the ultimate debtor and/or ultimate creditor fields of a payment message. Importantly, the concept of OBO payments should not be applied when the payment is "on behalf of" another PSP – this is a correspondent relationship and should be treated as such, as illustrated below.

Under the OBO scenario related to a payment factory function, the factory within the corporate entity pays or collects on behalf of other entities within the group. Prior to allowing corporate entities to make payments on behalf of other parties, these arrangements must be understood by the debtor agent PSP to ensure the OBO relationship is permissible under local regulation, e.g. regarding custodial or fiduciary relationships. In the scenario of a law firm or similar legal entity that often represents third parties, the transaction initiated by the legal entity (who is the customer of the law firm or similar legal entity) is on behalf of its customer, who is the ultimate debtor. The legal entity is not itself a PSP, but it is using its account with the debtor agent PSP to conduct a transaction on behalf of a third party who is not a customer of the debtor agent PSP.

These scenarios are distinct to a situation where a PSP maintains another PSP as a customer, and processes transactions received from the customer PSP on behalf of its underlying customers. In this case, there is a clear "debtor agent PSP" who initiates the payment, which is then processed by the "intermediary agent PSP" who maintains the PSP as a customer (the relationship-owning PSP), and all roles and responsibilities as identified in these revised Standards should apply. This type of flow is not the same as an OBO scenario, and rather is akin to a correspondent relationship. Further, under such correspondent relationships, it is important to distinguish PSPs that are appropriately licensed and registered with the local regulatory authority to conduct payment services, versus legal entities that may be acting as a PSP without required licenses/registrations in the local market. For instance, a PSP with global operations may be licensed/registered in their home jurisdiction (among others), but may not have the required licenses in the local jurisdiction in which the payment account is held.

D. In order to support payment transparency for the OBO scenarios identified above (e.g. in the case of the payment factory or the law firm), when the debtor agent PSP's customer is making payments on behalf of an "ultimate debtor", the debtor agent PSP should:

- Undertake sufficient CDD on its customer to confirm to a reasonable degree that payments for OBO parties are consistent with the line of business/expected activity of the customer.
- Set out in its policy what ultimate debtor/originator information should be provided by its customers, and clearly communicate those expectations to its customers.
- To the extent identifiable from the customer instructions, and practically achievable given the message format used by the PMI, include the full name and address of the ultimate debtor in addition to that of the debtor agent PSP's customer in the payment message. Information about the ultimate debtor may be more relevant for financial crime compliance purposes than customer information in this scenario. The name and address will not be subject to verification and the PSP should pass on the name and address as supplied by its customer.
- Where neither ultimate debtor nor customer (i.e. debtor) information can be provided (due to limitations in the number of fields and/or their length) in the same payment message, the PSP should set out in its policy whether to provide information on the debtor, as detailed in sub-section (A.) above, instead of providing information on the ultimate debtor. These policies must be in line with the regulations of the applicable jurisdictions for the PSP as well as the requirements established by the correspondent intermediary agent PSP (when applicable) that will facilitate the settlement of the payment for the debtor agent PSP's benefit (i.e. the relationship-owning PSP).
- Be prepared to source and share additional information on the debtor or ultimate debtor to other PSPs in the payment chain when requested.

The debtor agent PSP should maintain a clear position in policy where they permit OBO transactions based on customer type and underlying business models. This will enable the PSP to embed appropriate controls for the oversight and monitoring of such OBO transactions, including whether the business model fits within expected OBO type payments and whether ultimate debtor information is provided to the PSP on a regular basis.

4. Intermediary agent PSPs

The intermediary agent PSP is responsible for:

- Ensuring compliance with its own local laws and regulations, including (if applicable) the rulebook for the PMI through which the intermediary agent PSP intends to facilitate settlement of the payment, as well as FATF Recommendation 16 to the degree permissible if there is a difference in requirements and recommendations.
- Maintaining risk-based policies and procedures to determine when to execute, reject or suspend a payment in line with the PSP's applicable AML/CTF and sanctions compliance obligations.
- When applicable under a correspondent relationship, conducting full CDD on the PSP customer whose payments it processes, in line with correspondent banking due diligence principles[14], and other PSP customer-related requirements as the relationship-owning PSP. This should include, on a risk-based approach:
    - confirming that the payment model as proposed by the PSP customer is executed correctly in practice; and
    - confirming that the use of distinct payment approaches or permitted exceptions (e.g. in pursuing bundled payments, collection agent models, or "goods or services" provisions) are in line with the policies established by the intermediary agent PSP as agreed at onboarding.
- Passing on complete information that is received within payment messages, to the fullest extent permitted by the relevant PMI, to the next PSP in the payment chain.
- Monitoring, based on information provided in the payment message, its PSP customer's payment activity to identify potentially suspicious activity or to enforce sanctions compliance, unless monitoring is not required by applicable regulations.
- Retaining a record of all the information received from the debtor agent PSP or, if applicable, the previous intermediary agent PSP now instructing the payment through the intermediary agent PSP.

Importantly, although the intermediary agent PSP may be responsible under applicable law for ensuring that the required fields have been completed for both the debtor and the creditor, the intermediary agent PSP is **not** responsible for:

- Conducting CDD on debtor or intermediary agent PSPs with whom the intermediary agent PSP does not hold a correspondent or similar relationship.
- Conducting CDD on any creditor agent PSP with whom the intermediary agent PSP does not hold a business relationship.
- Identifying, or otherwise conducting CDD on, the underlying customers of the debtor agent PSP, any other intermediary agent PSP or the creditor agent PSP.
- Identifying whether payments that it processes are bundled or to seek to unbundle such payments that it may learn are bundled.
- Determining if the debtor agent PSP or any intermediary agent PSPs not immediately previous in the payment chain have correctly applied the permissible criteria established by the relevant competent authority for bundled payments (e.g. "many-to-many" scenarios), for payments operating via a collection agent model, for payments considered as "goods or services", or for any other payment types outside of the scope of payment transparency regulation.

[14] See Wolfsberg Financial Crime Principles for Correspondent Banking

5. Creditor agent PSPs – beneficiary institutions/payee PSPs

The creditor agent PSP is responsible for:

- Ensuring compliance with its own local laws and regulations, including (if applicable) as a participant in the PMI through which the creditor agent PSP intends to facilitate settlement of the payment for its customer, the creditor.
- Maintaining risk-based policies and procedures to determine when to execute, reject or suspend a payment in line with the PSP's AML/CTF and sanctions compliance obligations.
- Identifying, verifying, and conducting full CDD on its customer (the creditor), as well as related record keeping.
- Instructing the creditor on the appropriate usage of virtual reference number[15] compound naming when giving settlement instructions to counterparties, e.g. to ensure that when virtual reference numbers are allocated to specific parties, those counterparties do not replace the true account creditor (e.g. in merchant acquiring or collection on behalf of scenarios).
- Determining, based on the information available in the payment message, if the payments received by its customers represent potentially suspicious activity or violate applicable sanctions programmes.

The creditor agent PSP is **not** responsible for:

- Conducting CDD on the debtor, debtor PSP, or any intermediary PSPs, given that the creditor agent PSP is acting on behalf of the creditor.
- Determining if the debtor agent PSP or any intermediary agent PSPs in the payment chain have correctly applied the permissible criteria established by the relevant competent authority for bundled payments, for payments operating via a collection agent model, for payments considered as "goods or services", or for any other payment types outside of the scope of standard payment transparency regulation.

Going forward

In December 2019, the Group published a Statement on Effectiveness[16] that outlined what it believes are the key elements of an effective AML/CTF programme (The Wolfsberg Factors):

1. Complying with AML/CTF laws and regulations.
2. Providing highly useful information to relevant government agencies in defined priority areas.
3. Establishing a reasonable and risk-based set of controls to mitigate the risks of an FI[17] being used to facilitate illicit activity.

Complying with AML/CTF laws and regulation is a commitment that must apply to any provider of payment services. Today, payments can be originated by entities that are not banks, expanding the set of "gate-keepers" to the financial system. It is the debtor agent PSP originating the payment – bank or non-bank – that is uniquely positioned to ensure that the payment provides the maximum required level of transparency at its outset. Thus, the principal responsibility for ensuring payment transparency compliance begins with the debtor agent PSP.

[15] A virtual reference number – also at times referred to as "virtual account number", "virtual International Banking Account Number (vIBAN)", "virtual identification number", "virtual receivables number" or "virtual bank account" – is a reference number issued by a PSP to allow the tracking of incoming payments. A unique bank account may have multiple virtual reference numbers linked to it. A virtual reference number is typically linked to a unique bank account.
[16] The Wolfsberg Group – Statement on Effectiveness
[17] While "FI" is used in the original, PSP is appropriate in the context of this paper.

Providing highly useful information to relevant government agencies is not possible if the payment message does not include basic data on debtor and creditor parties (and any intermediaries). Required information must be structured appropriately and verified when required by regulation. When lower levels of transparency are permitted under existing regulation, competent authority expectations on identifying suspicious activity or enforcing sanctions compliance must adjust. Intermediary agent PSPs, and to some extent creditor agent PSPs (the beneficiary institution), are often unable to meet monitoring and sanctions compliance expectations when legally permitted bundling, or collection agency models, or the application of "goods or services" provisions, can be initiated and settled with limited underlying information on the debtor and/or creditor as the necessary information is not present in the payment.

The challenges associated with payment transparency cannot be resolved solely by payment and compliance specialists within banks, but rather require agreement among all payments stakeholders – including competent authorities, the PMIs within their countries, and non-bank entities that provide payments – to understand how the increase in payment actors and associated payment methods redistributes accountability across the financial system in addressing financial crime risk.

The revised Wolfsberg Payment Transparency Standards, supplemented with the visual aid of payment diagrams (see Appendix A) illustrating the complexity and associated transparency challenges experienced by PSPs in today's world, aim to build this consensus in line with an effective financial crime compliance programme.

APPENDIX A: Payment Flow Diagrams

As highlighted throughout these Payment Transparency Standards, the Group notes the fast-moving pace of payment innovation, with often blurring lines between when a payment starts and ends, and the multitude of actors that may be involved in moving funds. Payment chains are often highly intermediated, with cross-border payments broken down into a series of distinct domestic and cross-border transfers. For illustrative purposes, the Group has provided several non-exhaustive examples of how a payment, or a series of payments, may cross borders. The payment diagrams serve to highlight the challenges that confront PSPs and cover a range of scenarios, with varying levels of payment intermediation and payment actors involved in the movement of funds, as follows:

Diagram 1 Person-to-person payment flow: Cross-border payment between two individuals using two PSPs with no intermediaries.

Diagram 2 Correspondent banking: Cross-border payment via an intermediary agent PSP.

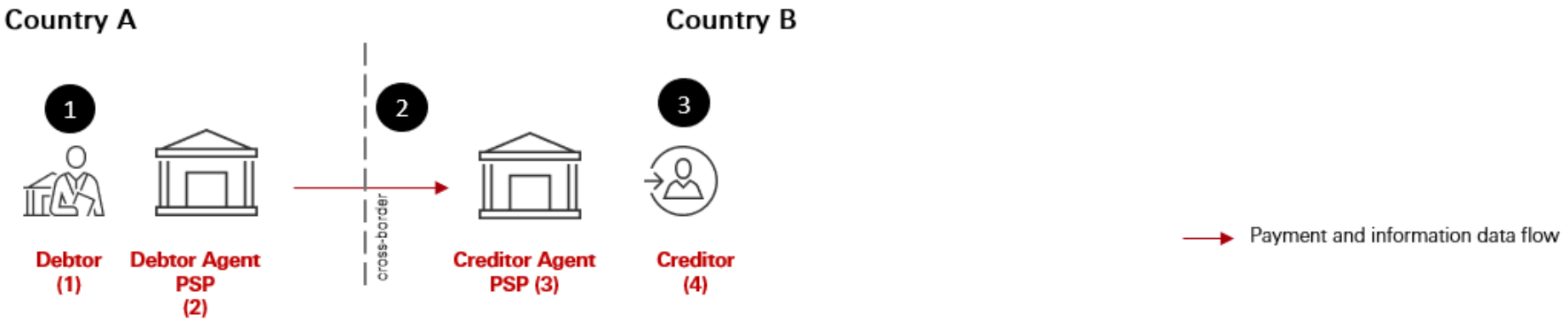
Diagram 3 Payment processor: A PSP processing card payments on behalf of its customers (merchants).

Diagram 4 Money remittance: Cross-border money remittances effected using an intermediary agent PSP, to be disbursed via local bank transfers to creditors.

Diagram 5 Money remittance with cash pay-outs: Cross-border money remittances effected using a network of intermediary agent PSPs, to be disbursed to creditors via cash pay-outs or local bank transfers.

This section will conclude with a summary of the payment transparency challenges (and limitations) that a PSP will face in such situations.

Diagram 1 Person to person payment flow: Cross-border payment between two individuals using two PSPs with no intermediaries

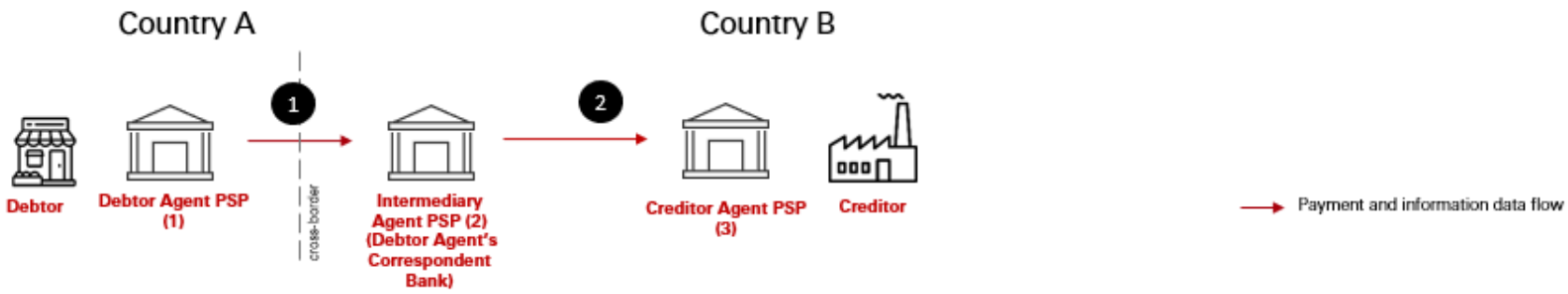


Summary of payment flow & payment transparency challenges:

1. An individual (debtor) in Country A needs to make a payment to an individual (creditor) in Country B.
2. The debtor agent PSP (2) takes the funds from the debtor's account and transfers them directly to the creditor agent PSP (3). The creditor agent PSP (3) receives the transfer from the debtor agent PSP (2). To effect the cross-border payment, the debtor agent PSP and creditor agent PSP will either have a direct account relationship with each other or be connected as common members of a cross-border PMI.
3. The creditor agent PSP credits the creditor's account.

The transaction poses few payment transparency challenges, provided full details are submitted by the debtor and passed from debtor agent PSP to the creditor agent PSP.

Diagram 2 Correspondent banking: Cross-border payment via an intermediary agent PSP

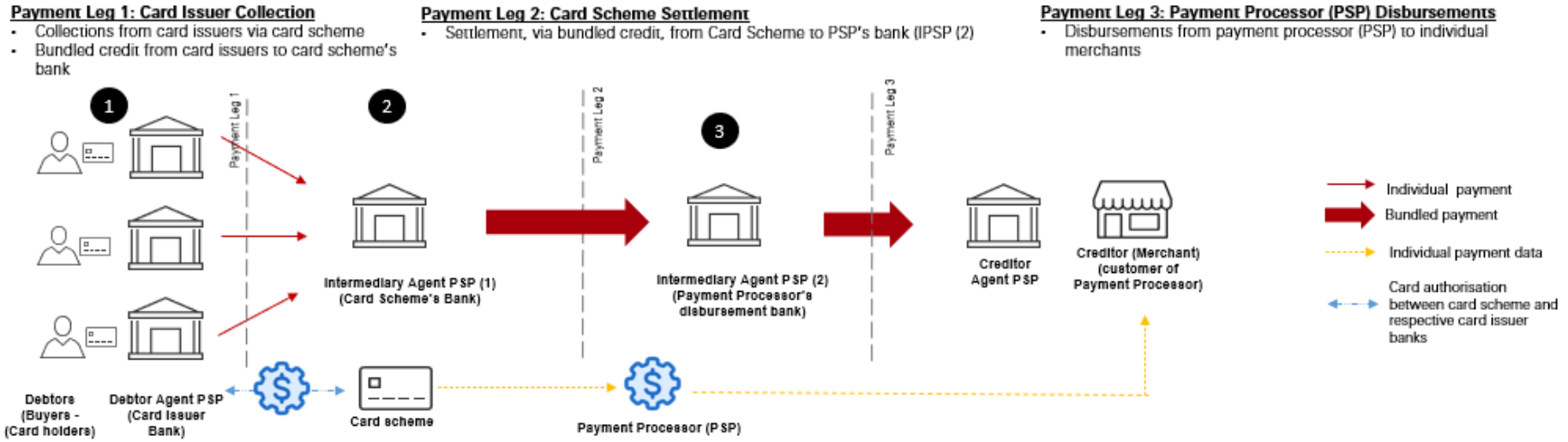


Summary of payment flow & payment transparency challenges:

1. A furniture shop (debtor) in Country A needs to make a single payment to its furniture supplier (creditor) in Country B. The debtor instructs its bank (debtor agent PSP) to send money to the creditor in Country B. As the Debtor Agent and Creditor Agent do not share a direct relationsip, the debtor agent PSP (1), a local bank in Country A, takes the funds from the debtor's account and instructs its intermediary agent PSP (2), or "IPSP" (2), in Country B to send the money to the creditor agent PSP (3).
2. The single payment is made from intermediary agent PSP (2) to the creditor agent PSP (3). The creditor agent PSP (3) receives the single payment with full debtor information.

The transaction poses few payment transparency challenges, provided full details are submitted by the debtor and passed from the debtor agent PSP to the creditor agent PSP, via the intermediary agent PSP.

Diagram 3 Payment Processor: A PSP processing card payments on behalf of their customers (merchants)



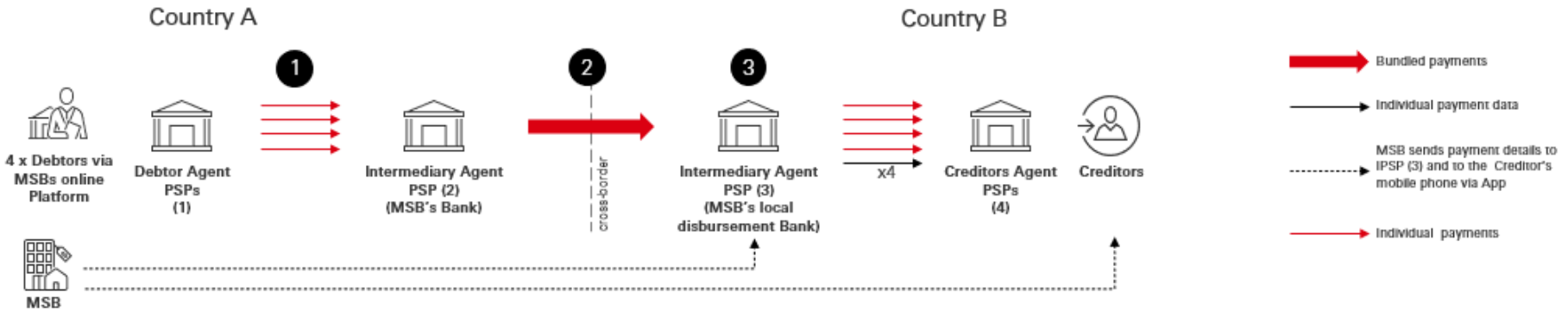
Summary of payment flow & payment transparency limitations (permissible under FATF 16):

Within this model, the transaction data resides within the card scheme. The two bundled transfers do not contain card scheme data and the PSPs in this scenario do not see the underlying customer details/transactions. Lower levels of payment transparency may be permitted under local regulations, as such transactions using a payment card will be viewed as transactions between a merchant and its end customers for the purchase of goods or services.

1. Card Issuers use their National Net Settlement Scheme to transfer in a bundle of all their customers' transactions to the Card Scheme's bank account, IPSP (1). Card Issuers are repaid by the Card Holder's bank account.
2. The Card Scheme transfers from their bank account at IPSP (1) the settlement of all funds from the Card Issuers to the Payment Processor's disbursement bank, IPSP (2).
3. IPSP (2) disburses the required amounts to the individual merchant's bank account with the creditor agent PSP. There is limited transparency in payment leg 3 in so far as the merchants receiving the payments, though not the debtors making the payments, are visible to the Intermediary Agent PSP.

Note: This illustrates a basic payment flow, it does not represent the end-to-end card scheme payment cycle.

Diagram 4 Money remittance: Cross-border money remittances effected using an intermediary agent PSP to be disbursed via local bank transfers to creditors



Summary of payment flow:

1 Individuals (debtors) in Country A log onto their MSB account and enter their respective payment instructions to send money to named parties (creditors) in Country B. Each debtor funds the transaction with a bank transfer from their own bank (debtor agent PSP 1) via a single, domestic payment made from the debtor agent PSP (1) to the MSB who maintains an account with intermediary agent PSP (2), or "IPSP" (2). For the debtor agent PSP (1) and IPSP (2), the domestic payment may be subject to sanctions screening, depending on local regulations. The MSB has the underlying details received from its debtor/customer and will be aware that it is facilitating a cross-border remittance; thus, it needs to conduct sanctions screening and adhere to applicable regulatory requirements for a cross-border payment.

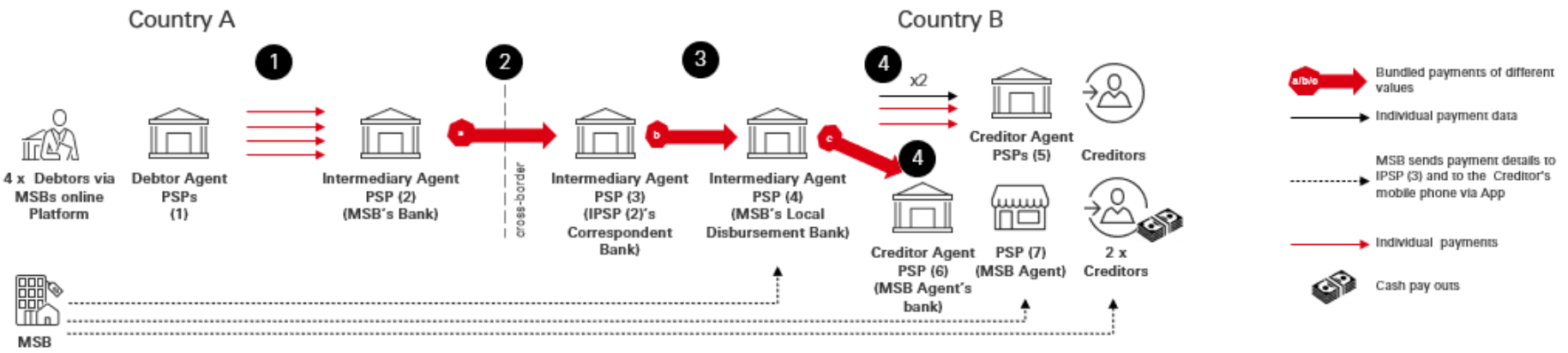
2 IPSP (2) makes a bundled payment to IPSP (3), which is the MSB's local disbursement bank in Country B. The bundled payment may be *a)* an aggregation of payments received from multiple debtors to be disbursed in Country B to the respective creditors, *b)* treasury settlement effected by the MSB between the two countries, or *c)* combination of *(a)* and *(b)*. Simultaneously, the MSB sends a payment data file with the names, bank and account numbers of the creditors and details of payment to IPSP (3) in Country B.

Payment transparency challenge: IPSP (2) and (3) do not know if the funds being transferred and received by them respectively are for *(a)*, *(b)* or *(c)*. However, irrespective of the purpose of the funds transfer, the MSB in Country A is the customer of IPSP (2), and the underlying debtors of the MSB do not become the customers of IPSP (2) for the purpose of applicable laws and regulations. The same applies to IPSP (3), i.e. that the MSB in Country B is the customer of IPSP (3) and the underlying debtors of the MSB do not become the customers of IPSP (3). There is no requirement or expectation on IPSP (2) and (3) to unbundle the payment.

3 IPSP (3) receives the payment data file from the MSB to make individual payments to the respective creditor agent PSPs. The creditor agent PSP (4) receives the single payment from IPSP (3) and credits the payment into the creditor's bank account. While the final disbursement will be an individual

payment to the creditor, the payment may be seen as domestic and not cross-border by creditor agent PSP (4), unless the final payment message clearly indicates that the debtor agent and/or IPSP (2) original account location was in Country A not Country B.

Diagram 5 Money remittance with cash pay-outs: Cross-border money remittances effected using a network of intermediary agent PSPs, to be disbursed to creditors via cash pay-outs or local bank transfers



Summary of Payment Flows

1 Individuals (debtors) in Country A log onto their MSB platform and enter their respective payment instructions to send money to named parties (creditors) in Country B. Each debtor funds the transaction with a bank transfer from their own bank (debtor agent PSP). This is a single, domestic payment made from the Debtor Agent PSP to the MSB who maintains an account with the intermediary agent PSP "IPSP" 2. Similar to Diagram 4, for the debtor agent PSP and Intermediary Agent PSP (2), the domestic payment may be subject to sanctions screening depending on local regulations. The MSB who has the underlying details received from its debtor/customer and is aware that it is a cross-border remittance, it will need to conduct sanctions screening and adhere to applicable regulatory requirements for a cross-border payment.

2 The MSB receives the payment information from the respective debtors via its online platform, aggregates the payments with other funds going to Country B and instructs its Bank (IPSP (2)) to send a bundled payment to its local disbursement bank, IPSP (4), in Country B. The bundled payment may be *a)* an aggregation of payments received from multiple debtors to be disbursed in Country B to the respective creditors, *b)* treasury settlement effected by the MSB between the two countries, or *c)* combination of *(a)* and *(b)*. To make the cross-border payment, IPSP (2) sends a bundled payment via its correspondent bank, IPSP (3) in Country B. Note that the bundled payment sent by IPSP (2) may not be the same value as the bundled payment sent by the MSB to IPSP (4) – the bundled payment sent by IPSP (2) may be a separate value determined by IPSP (2) to best suit its operational, treasury forecasting, and/or foreign exchange needs.

The same payment transparency challenges presented in Diagram 4 apply to Diagram 5; compounded by the presence of an additional intermediary agent (IPSP (3)). Similar to Diagram 4, there is no expectation for the IPSPs to unbundle the payment, or regard the underlying debtors/customers of the MSB as customers of IPSP (2) and (4).

3 IPSP (3) receives the bundled payment and makes a separate bundled payment to the MSB's local disbursement bank, IPSP (4), in Country B. The payment data is sent by MSB to IPSP (4) in Country B to facilitate the local disbursement of funds.

4 IPSP (4) reconciles the bundled payment received to the data received from the MSB and credits the respective creditors' accounts held with the creditor agent PSPs (5) and to the MSB agent's bank, i.e. creditor agent PSP (6). With the funds credited into creditor agent PSP (6), the creditor will be able to go to MSB agent PSP (7) to pick up cash with the details received via their mobile phone. As the customer relationship is held with the MSB and not with the MSB agent (who is acting as the disbursement agent), the applicable laws and regulations and enforcing sanctions compliance will apply to the MSB. While the final disbursement will be an individual payment to the creditor, the payment may be seen as domestic rather than cross-border by creditor agents PSP (5) and (6), unless the final payment message clearly indicates that the debtor agent and/or IPSP (2) original account location was in Country A not Country B.

Payment Transparency Challenges (and Limitations)

As set out in the payment diagrams and described in the Standards, payments can be highly intermediated and involve different types of payment actors in the pursuit of faster and cheaper payments. These payment flows can pose varied payment transparency challenges to PSPs not least because of limitations in the information that each may receive. Those challenges (and limitations) impact how PSPs are able to fulfil their monitoring and sanctions compliance obligations, in accordance with the role(s) they play in the payment chain. Key payment transparency challenges and limitations include but are not limited to:

1. Limited Payment Transparency: payment diagrams 4 and 5 highlight that only the debtor agent PSP, in that case the MSB, will have the full visibility of the underlying debtors/creditors, their respective addresses, and purpose of payment. For varying reasons (e.g. bundling of remittances, limitations in the local payment scheme to carry all the information received with a transfer), that underlying information is not made available to all the downstream PSPs for them to perform (or know they need to perform) sanctions screening on the transactions and conduct effective transaction monitoring. Furthermore, while the MSB can monitor and file Suspicious Activity/Transaction Reports (SARs/STRs) in its own jurisdiction, the cross-border risks may not be shared with the other parties in other jurisdictions involved in the payment chain, thereby impacting their ability to take appropriate risk mitigation measures. The competent authorities and law enforcement agencies in intermediary and receiving jurisdictions may also be unaware of the cross-border nature of the transaction.

2. Bundled Payments: closely linked to Point 1, bundled payments (which occur for a number of reasons, e.g. treasury settlement, foreign exchange conversion, and operational and cost efficiency purposes) result in reduced payment transparency to the downstream PSPs. Intermediary PSPs may not know that they are processing a bundled payment and not all PSPs who do know will, or will choose to[18], request and obtain the full underlying debtor/creditor information for them to monitor and sanction screen the transactions. Notwithstanding this and subject to applicable laws, PSPs should cooperate as fully as practicable with other PSPs in the payment process when requested to provide information about the parties involved.

3. Ambiguity as to when a payment starts and ends: this is increasingly blurred as a single payment may be initiated in one jurisdiction by an individual to be sent cross-border, then bundled with other payments also to be sent cross-border via a series of domestic and correspondent type funds transfers. This is typically to achieve faster and cheaper payment settlement and is made possible by the breaking down of cross-border payments into domestic payments and disbursements processed using domestic PMIs, and a separate bundled cross-border payment***.*** As such, it is challenging for IPSPs to determine if the intent of the payment they are processing is domestic or cross-border, bundled or treasury (or both) when the IPSPs do not have full visibility of the underlying creditor/debtors. This limitation should be reflected, and calibrated, into supervisory expectations and subsequent examinations.

4. Multiple PSPs/types of PSPs involved in the movement of funds: the multiple PSPs and the different business models may present heightened financial crime risks if payment transparency obligations, and associated compliance requirements, are not well understood and undertaken by each PSP. Each PSP in the payment chain will need to meet, and be held accountable for, their regulatory obligations depending on the role that they play in the payment chain. Note that PSPs are **not** responsible for conducting CDD on debtors/creditors with whom they do not have a customer relationship e.g.

[18] The decision to screen the underlying debtors/creditors should be determined by the PSPs, on a risk-based approach, based on the role that they play in the payment chain.

intermediary agent PSPs are not responsible for performing CDD on the debtors/creditors (who are customers of the debtor agent PSP and creditor agent PSP respectively). This distribution of accountability across all PSPs in the payment chain will need to be reflected, and calibrated, into supervisory expectations and subsequent examinations.