



9 September 2024

Financial Stability Board
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Subject: Response to the Financial Stability Board's (FSB) Consultations on Regulating and Supervising Cross-border Payment Services and Data Frameworks Alignment

Dear Sir or Madam,

The Wolfsberg Group (the Group) welcomes the opportunity to provide feedback on the FSB's recent consultations: (1) Recommendations for Regulating and Supervising Bank and non-bank Payment Service Providers Offering Cross-border Payment Services, and (2) Recommendations to Promote Alignment and Interoperability Across Data Frameworks Related to Cross-border Payments.

Our response addresses both consultations.

We recommend that the FSB address financial crime prevention holistically as well as prudential oversight in the consultative process. It is critical that any regulatory framework governing cross-border payments takes appropriate consideration of anti-money laundering (AML), counter-terrorist financing (CTF), counter-proliferation financing, fraud prevention, tax regulations, and sanctions compliance. Such a holistic approach should consider the regulatory requirements across these critical areas thoroughly, as they have a significant impact on the efficiency and security of cross-border payments.

The Group commends the FSB for proposing the establishment of a cross-border payment forum that includes private sector input and we urge that the role envisaged for the private sector be meaningful and substantive. While this proposal is specific to the Data Frameworks consultation, we believe that private sector input would also be beneficial in the evolution of the Regulatory and Supervisory environment. It is essential that the private sector's expertise and experience are integrated into the decision-making process to ensure that the proposed frameworks are both practical and effective.

We recommend strongly that the FSB call upon the Financial Action Task Force (FATF) explicitly to take appropriate action where Recommendation 16 is not applied consistently to all participants in the cross-border payments ecosystem. The FATF's role should be emphasised beyond being one of the 'competent authorities,' as consistent application of its recommendations is crucial for maintaining the integrity of cross-border payments.



The Group would like to challenge the assertion that there are no comprehensive international standards for regulating Payment Service Providers (PSPs)¹ and the cross-border services they offer. Existing FATF Recommendations and the Group's guidance each cover significant aspects of this area, and we encourage the FSB to collaborate with the FATF on international standards covering cross-border payments and their consistent implementation. We urge the FSB to acknowledge and build upon these existing frameworks rather than implying a standards vacuum. We concur that achieving international alignment in approach and standards can help address several of the challenges highlighted provided they are applied consistently and take a 'same business, same risk, same rules' approach. We believe that the root cause of many of these challenges lies in the translation, interpretation and inconsistent application of FATF Recommendations into domestic law and regulatory supervision. Therefore, for any international approach to be truly effective, it must consider and align with the FATF Recommendations. We would also like to draw your attention to the standards released by the Group in support of the fight against financial crime, specifically the 2023 Wolfsberg Payment Transparency Standards.²

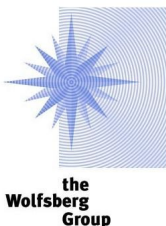
Transparency of the cost and time required for a payment to reach its creditor is important, but it represents only part of the broader picture. Transparency also extends to what information is required to be transmitted within the payment itself. Increased requirements for information to be conveyed in a payment should be considered carefully in the design of any new framework as this can lead to delays and/or obstacles as PSPs fulfil their regulatory responsibilities.

The Group would like to draw the FSB's attention to the fact that innovation has driven the emergence of alternative methods for moving funds across borders, with non-bank PSPs leveraging domestic payment market infrastructures (PMIs) for certain segments of a cross-border transaction. Non-bank PSPs may use a combination of internal net settlement, cross-border payments, and domestic PMIs to facilitate payment offerings to customers. To ensure a comprehensive regulatory coverage of cross-border payments, the FSB's efforts must address the use of these domestic methods and their integration into the broader payment ecosystem. In this context, we note the following passage in the FSB's consultation publication:

"The crucial role of banks in cross-border payments is further exemplified by the functions they perform in wholesale cross-border payments, wherein they facilitate large-value transactions between financial institutions, and which creates additional responsibilities in liquidity management and risk mitigation with respect to credit, liquidity, and currency risk. Therefore, banks are generally expected to implement robust

¹ 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.

² [Wolfsberg Group Payment Transparency Standards](#)



risk management strategies to safeguard the integrity of wholesale payment systems and are subject to comprehensive regulatory and supervisory standards.”

We agree and would highlight that this concern also extends to non-bank PSPs. Many of these are global entities managing substantial balance sheets and facilitating significant financial transactions including cross-border transfers, yet they do so without consistently being subject to the same rigorous level of regulation and supervision as traditional banks.

We strongly support the principle of ‘same business, same risk, same rules,’ which is vital for achieving a level playing field. The term ‘same rules’ must include the same prudential as well as AML/CFT regulation and supervision and be distinguished from ‘similar rules’, as the latter could open the door to regulatory arbitrage and undermine efforts to create an equitable environment for all market participants (i.e. banks, non-bank PSPs, and VASPs).

The fact that banks disproportionately assume risks when processing payments for non-bank PSPs should be addressed by aligning the regulatory standards for all entities that process payments. Irrespective of whether non-bank PSPs have direct or indirect access to payment systems, we believe that indirect scheme participants, such as non-bank PSPs initiating payments through direct participants (i.e. banks) should be subject to the same regulatory standards and supervision as those imposed on direct participants. Without consistent regulation and supervision, the responsibility falls disproportionately on banks to be held accountable for transactions initiated by these indirect participants. Banks will continue to apply their own risk assessments to non-bank PSPs, and these entities will still likely be subject to Enhanced Due Diligence³. With aligned regulatory and supervisory standards, banks may become more receptive to providing banking services to these non-bank PSPs, potentially leading to a reduction in instances of de-risking (which could range from declining/exiting PSP relationships to limiting the range of services provided).

These considerations go hand-in-hand with licensing requirements to handle payments and what that licensing means (i.e. giving clarity about what financial crime risk management obligations accompany the issuance of the licence), which would further aid in the effort of ensuring a level playing field.

The challenges associated with payment intermediaries, including the intermediary’s limited visibility of payment data and its impact on speed (i.e. requiring an intermediary to seek information which is not contained in the payment will cause delay), require careful consideration. The Group recommends that the practice of bundling payments is acknowledged and accounted for by standard setters and regulators. The Group believes that the solution is not to require payments to be unbundled (which is confirmed also

³ This is because processing a cross-border transfer for a PSP is the same business, posing the same risk and subject to the same treatment under FATF Recommendations that identify cross-border transfers in a correspondent banking context as high risk. See FATG [Guidance on Correspondent Banking Services](#) page 9.



in the latest European Banking Authority “Travel Rule” Guidelines⁴), as this would ultimately impose additional costs on consumers and could have an adverse impact on the speed of payments. Instead, the focus should be on recognising and assessing the risks associated with cross-border payments that are divided into separate payment legs, which can lead to increased fragmentation and reduced payment transparency. To manage these risks effectively, all PSPs—whether bank or non-bank—must be regulated to the same standards based on the activities they undertake and there should be clear roles and responsibilities for parties within the payment chain as they relate to bundled payments.

The ability of banks to identify suspicious activity and/or conduct transaction screening may be diminished where the information accompanying a payment is limited (particularly in a bundled transaction). This is a cause for concern within the banking community and may lead to de-risking by a bank if it considers it may be held liable for financial crime issues or that it is unable to maintain an effective control framework to manage the risks of its relationship with the non-bank PSP to the standard expected by its regulators. To address this, we stress the importance of equivalence in regulatory standards and supervision for all PSPs (banks or non-banks) based on the activities they undertake. This is crucial to ensure that financial crime risks are being effectively managed across the entire payment ecosystem, by all PSPs.

We would also like to share our view that the role of messaging systems in transferring payment data is crucial. It is important to align payments and messaging systems to the ISO20022 standard, especially in payment chains using different PMIs since a payment flowing across different PMIs may be subject to abbreviation or truncation if it flows from a PMI that can hold more information to a PMI that can hold less. We emphasise that adopting the ISO20022 format in a ‘like-for-like’ manner is insufficient to benefit from the new standard fully. The required information must be formatted in strict accordance with the ISO standard, and the use of the ISO standard should be strongly encouraged with PMIs tasked to identify appropriate technological enhancements to support the consistent and correct population of data via adoption of structured message fields, as such enhancements are reasonably practicable.”

We disagree with the FSB’s decision to exclude PMIs and Financial Market Infrastructures (FMIs) from the scope of the recommendations. If these infrastructures cannot support the necessary information, competent authorities and the relevant PMIs/FMIs should issue guidance on what the PMI should and should not be used for. Such technical limitations pose a challenge for all PSPs to comply with relevant payment transparency regulatory requirements and expectations. To ensure that PMIs and FMIs provide an appropriate infrastructure, it is crucial to recognise their role as gatekeepers in the payment ecosystem. Clear and more consistent global scheme rules must be established for cross-border eligibility and payment models to maintain the integrity and efficiency of these systems. For more detail in this area please refer to the Wolfsberg Group’s Payment Transparency Standards (see, for example, Chapter 1 “The PMI(s) and the competent authority(ies)”).

⁴ [Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation \(EU\) 2023/1113](#)



The Group recommends that the FSB considers sanctions risk as a material factor in cross-border payments (noting that sanctions are mentioned only once in the 'Cross Border Payments Frictions and Risks' section of the Regulating and Supervising consultation). Given the strict liability imposed by OFAC and OFSI, and the necessity of screening against lists issued by the EU, HM Treasury, UN etc for sanctions compliance—which results in friction and delays—a lasting solution can only be achieved through public sector action.

We question the emphasis on the use of Legal Entity Identifiers (LEIs) in retail payments. Instead, we suggest that the FSB considers terms like P2P (person-to-person), P2B (person-to-business), B2P (business-to-person), and B2B (business-to-business) to better categorise payments and assess the applicability of identifiers. Some may interpret 'retail payments' to be limited to P2P hence the irrelevance of LEIs to transacting parties (as opposed to their PSP) in this segment as opposed to P2B or B2B where identifiers have greater relevance.

The increasing use of virtual currencies⁵ and Virtual Asset Services Providers (VASPs) in facilitating cross-border transfers of value cannot be overlooked and we urge the FSB to consider the implications of this growing trend within the scope of its recommendations. The FSB's scope should encompass transfers of funds or value more broadly, rather than being limited to traditional fiat payments through PSPs. We believe that excluding virtual currencies would be a significant oversight given that virtual currencies and modern payment methods are increasingly intertwined, with both fiat and virtual currencies playing roles in cross-border transactions (a fact that has also been recognised by the EU Funds Transfer Regulation, which expressly applies to crypto asset services providers). For example, banks may facilitate fiat on-ramp to virtual currency exchanges on behalf of their retail customers, who then use virtual currencies for cross-border transfers or to cash out in another jurisdiction. Given that VASPs are still unevenly regulated, it is essential that they be included within the scope as non-bank PSPs since they are in the same business and subject to the same risks when transferring value. If the FSB omits these entities, it risks overlooking a substantial and growing segment of the payments industry and could have significant financial crime implications and lead to further de-risking. The Group acknowledges that the FSB may wish to consider additional recommendations or guidance specific to virtual currencies to address unique or evolving risks that may warrant additional evaluation by subject matter experts. However, the complexity, lack of understanding, and insufficient supervision of these modern cross-border payment methods mean that they should be factored into any comprehensive regulatory framework at the earliest opportunity. This approach would also be consistent with the principle of 'same business, same risk, same rules.'

⁵ In this context by "virtual currencies" the Group refers to a sub-category of digital assets used to transfer value. A digital asset is a cryptographically secured digital representation of value or rights and/or cryptographically secured token, recorded in digital form, that often relies upon the use of a form of distributed ledger technology (DLT) or cryptography and which can be transferred, traded or exchanged, and can be used for payment or investment purposes. See also FATF [Virtual currencies – Key Definitions and Potential AML/CFT Risks](#)



The consultations lack any reference to third-party payments, which is a critical omission. It would be beneficial to highlight the distinction between cross-border payments for third-parties as distinct from those made by PSPs that are proprietary in nature (though this may be the FSB's intent by defining its scope as retail payments). The highest friction in payment systems arises in third-party flows where the names and addresses of debtors and creditors along with details of payment information has to be screened for sanctions and other applicable risks. Therefore, there must be a clear differentiation between proprietary payments and third-party payments, especially considering that many net settlement arrangements, which may be categorised as proprietary or treasury operations, are effectively facilitating cross-border payments (despite being settled domestically). Specifically, we propose that the FSB consider these types of payments separately. The first category is for third party payments, featuring activity comprised of aggregating and facilitating the electronic transfer of third-party payment flows. The second category is for proprietary payments, where the PSP is transacting other than for the purpose of facilitating a payment for a third party.

To address this, the report should consider enhancing the sections on "Activity-Based Regulation" or "PSP Definition" by providing working examples of activities starting with third-party payments. This breakdown should then differentiate among various sub-segments, such as acquiring, marketplaces, peer-to-peer payments, and different payment instruments like e-wallets, and prepaid cards (stored value instruments).

We believe that the FSB's scope is too limited to adequately address the risks, controls, and friction within the payment ecosystem, as it only considers services offered to end users. By excluding an examination of how funds or value move from end to end—such as through non-bank PSPs, virtual currencies, virtual reference numbers⁶, bundling or netting—the FSB misses critical context for regulation, supervision, and oversight, as well as the risk-based decisions made by PSPs offering services to end users. If the FSB's ultimate goal is to recommend ways to reduce costs and friction for customers, it is crucial to consider the risks that arise throughout the entire end-to-end transaction process. These risks are likely to be the root cause of costs or friction, rather than the services being offered directly to end users. Additionally, as noted above, the FSB mentions a focus on retail payments without defining what this means. Cross-border payments may be made for retail customers and corporate customers (some of whose payments will be to/from retail customers), and the frictions being experienced are not limited to retail transactions. Instead, these issues form part of a much broader challenge affecting cross-border payments across both retail and corporate segments.

⁶ As noted in footnote 15 to the Wolfsberg Payment Transparency Standards '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.



Specific Recommendations in relation to the Consultations

Consultation on Regulating and Supervising Bank and Non-bank Payment Service Providers Offering Cross-border Payment Services:

Recommendation 1.

We recommend that risk assessments conducted by competent authorities concerning the cross-border payment sector be shared with the regulated sector. Providing corresponding guidance on the necessary control frameworks, such as the type of Customer Due Diligence, monitoring, and payment transparency requirements (categorised by relevant parties, e.g. debtor/creditor agent, intermediary), would be beneficial. These guidelines would support a risk-based approach and should also provide specific directions to manage identified risks effectively.

Additionally, it is important to highlight the risks associated with domestic PMIs being utilised for cross-border payments. This aspect needs to be explicitly addressed, as it carries unique financial crime risks that require attention.

As part of the ongoing risk assessment process, we suggest including an analysis of Suspicious Activity Reports (SARs) raised by different types of PSPs which can be analysed by competent authorities to highlight any concentrations of particular financial crime risk.

Lastly, we suggest that Recommendation 1 should be implemented first to inform subsequent recommendations will enhance the overall effectiveness of the proposed measures.

Recommendation 2.

The FSB should explicitly address the risks associated with cross-border payments that are broken into domestic legs, as well as other innovative cross-border payment methods, and provide guidance on how these risks should be managed. As business models evolve, it becomes increasingly challenging to determine the appropriate licensing and regulatory frameworks that should apply. Banks are often perceived as the primary entities responsible for compliance with payment transparency regulations. However, especially when cross-border payments are broken down into component flows (such as a domestic collection payment followed by the cross-border payment and finally a domestic disbursement), they have limited visibility over the end-to-end transfer of funds due to the introduction of intermediaries, virtual currencies and modern payment methods (such as bundled or netting-based systems) within the value transfer process.

This trend significantly increases risk and necessitates stronger controls. There is a need for a level playing field, a reassessment of accountabilities of all parties involved in the payment, and a stronger emphasis on cross-border data sharing among banks, non-bank PSPs, and Financial Intelligence Units (FIUs) to combat financial crime.



Given the limited visibility of banks who facilitate payment flows for non-bank PSPs into the underlying payment flows, especially as regards bundled payments it is crucial that non-bank PSPs are regulated and supervised to the same standards as banks for their payment activity to further mitigate financial crime risk. This alignment will help mitigate risks and ensure a more robust and compliant cross-border payment ecosystem.

The Group recommends that the FSB provide clear guidelines or expectations for countries to establish legal frameworks that facilitate the repatriation of funds (across all value transfer types, including virtual currencies), both domestically and cross-border, along with the necessary provisions for related information sharing. For instance, if victims are able to recover their funds or if law enforcement can identify and reclaim the proceeds of crime from the creditor agent PSP, even when located in a different jurisdiction, cross-border payments could potentially carry a risk profile more akin to domestic payments. This would mitigate the risks (especially fraud risks) associated with modern payment methods that often lack transparency and obscure the true cross-border nature of the transactions.

Recommendation 3.

Laws and regulations should ensure the consistent and proportionate application of sanctions policies, recognising the extraterritorial impact of some jurisdictions' sanctions regulations.

Recommendation 4.

We support the publication of guidance for a risk-based approach to payments and offer our Payment Transparency Standards⁷ as a valuable resource.

Competent authorities must provide clear and detailed guidance on the expectations for intermediaries within a payment chain, whether they are banks or non-bank PSPs. Specifically, it is important to define their obligations regarding screening and monitoring, particularly in scenarios where transactions are processed in bulk or through net settlement.

It is important to acknowledge that cross-border third-party payments, both for peer-to-peer transactions and payments for goods and services, rarely occur through single payments anymore. This evolving landscape often leaves intermediaries unable to identify the true debtor or creditor for these transactions. This reduces the effectiveness of monitoring conducted for financial crime risks and sanctions screening.

There is considerable concern within the banking community that banks might be held liable for sanctions or financial crime issues, given the limited visibility into the underlying activities (e.g. in bundled payments, in cases where the PMI is unable to carry all the relevant data, in situations where multiple intermediaries are present etc.) which in turn also reduces the effectiveness of monitoring and screening tools. This concern needs to be addressed as it represents a significant challenge for banks when they support cross-border payments, especially for non-bank PSPs, and can be done so by explicitly setting out the roles and

⁷ [Wolfsberg Group Transparency Standards](#)



responsibilities of all actors in a payment chain, particularly in cases where non-bank PSPs are the only ones with an end-to-end view of the payment flow. This shift in accountability should be integrated into supervisory examinations and expectations. Furthermore, non-bank PSPs should be regulated with the same rigour and standards as banks to ensure consistent oversight and risk management across the sector.

Recommendation 5.

We emphasise the need to review licensing and supervisory regimes, including existing exemptions, to ensure they remain fit for purpose and align with the evolving payment landscape. For instance, in some countries, many non-bank PSPs claim exemption from licensing under the commercial agent exemption, yet it is not always clear whether they do or should truly qualify for this. As highlighted in the consultations, while some countries adopt an activity-based approach and others an entity-based approach to regulation and supervision, the increasing complexity of non-bank PSPs' hybrid business models—offering a mix of services—makes it challenging to determine what licences they hold for specific services. In some jurisdictions, specific exceptions exist, but these too can be difficult to interpret given the intricate nature of modern business models.

The focus should extend beyond domestic licensing to consider whether a PSP licensed in one jurisdiction is permitted to conduct payment activities in another jurisdiction without obtaining a licence there. Some PSPs may not even recognise themselves as PSPs and therefore might not seek the necessary licences. We have also observed cases where small online companies, acting as PSPs, do not fully understand their licensing obligations, both domestically and cross-border. This issue is further complicated by requests for non-resident accounts to facilitate cross-border payments.

To address these challenges, providing worked examples or establishing a working group to clarify licencing requirements would be highly beneficial. There is often a lack of precision, clarity, or guidance from existing standards to help PSPs navigate licensing statuses (e.g. by not making clear the obligation that the non-bank PSP incurs alongside the right to provide payment services). Consequently, the responsibility frequently falls on banks to interpret the rules, which adds to the complexity and potential for misunderstanding.

Recommendation 6.

FIUs, along with banks and non-bank PSPs, must enhance cooperation and information-sharing to be more effective in addressing financial crime risks to the fullest extent permitted by applicable laws and regulations and laws and regulations may need to be changed to achieve this. The increasing prevalence of cross-border payments that are settled domestically has resulted in reduced transparency, making it harder for individual countries to grasp (or even identify the presence of) the associated cross-border risks fully. This shift is leading to a more siloed approach, where each country's visibility into cross-border activities is limited. Therefore, fostering cross-border cooperation is essential.



This also aligns with the broader objectives outlined in the FSB's data framework consultation, which emphasises the importance of global collaboration in addressing these challenges.

Consultation on Alignment and Interoperability Across Data Frameworks Related to Cross-border Payments: Consultation:

- Clarification is needed regarding the understanding of payee (creditor)/payer (debtor) distinctions on page 6 of the consultation.
- In general, we are supportive of the principle of including an LEI/BIC or unique official identifier to enhance the accuracy of identification information on relevant parties. In recognition that the current LEI adoption is mainly confined to large corporates in highly developed economies, we suggest that the FSB and other competent authorities make suitable allowances for a transition period for entities to adopt LEI and set out a clear explanation as to what financial crime compliance issues LEI are intended to solve. We believe that requiring LEI usage too soon will result in friction in global payments and raise financial inclusion barriers particularly for small and medium sized enterprises in less developed economies. In addition, similar to the point raised above, there needs to be a corresponding push from FSB and other competent authorities for list providers and relevant authorities to populate such BIC/LEI or unique official identifier information in their lists to maximise the effectiveness of requiring, and subsequently using, this information. As an example, from feedback given to us by third party vendors, a significant part of the challenge is to tie, definitively, the name on the LEI lists to a name on the sanctions list.
- The term 'non-standard technical solutions' for screening requires further elaboration.
- A distinction should be drawn between broad data (e.g. data held in a data centre) and narrow data (e.g. data within individual payments), as the challenges differ significantly.
- In addition to innovation in the payments business we encourage innovation in supervision, both by and in collaboration with regulators and supervisors.

Thank you for considering our input on these critical issues. We are eager to continue collaborating with the FSB to develop effective and comprehensive frameworks that address the challenges and opportunities in cross-border payments.

Yours sincerely,

Alan Ketley
Executive Secretary
The Wolfsberg Group