

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

Guidance on the Provision of Banking Services to non-bank Payment Service Providers

1. Introduction

This guidance document establishes the Wolfsberg Group's (the Group's) framework for managing the financial crime risks associated with non-bank payment service providers (non-bank PSPs). The guidance builds upon the Group's foundational work on correspondent banking, as well as the updated [Payment Transparency Standards](#) published in October 2023, and the accompanying [Wolfsberg Guidance on Payment Transparency - Roles and Responsibilities](#) published in 2024. This guidance also incorporates the June 2025 updates to the Financial Action Task Force's (FATF) Recommendation 16, aimed at enhancing transparency and security in cross-border payments by requiring complete originator and beneficiary information in wire transfers.

2. Scope

This guidance document uses the term non-bank PSP to capture the full spectrum of payment service providers that facilitate funds transfers while not holding a banking licence. This includes settlement of payments for goods and services, money remittances (domestic and cross-border), and transfers carried out using payment cards, electronic money instruments, mobile phones, or any other digital or IT-based prepaid or postpaid devices with similar characteristics. This may encompass money service businesses (MSBs) as well as entities commonly referred to as third-party payment processors (TPPPs), fintechs and electronic money institutions (EMIs).¹

¹ While the term "payment service provider" may be defined by regulators in different jurisdictions to include other entity types, the recommendations in this paper are based on the definition provided.

This guidance may also be of value for other types of non-bank PSPs, such as account information service providers (AISPs) or payment initiation service providers (PISPs).

The following entities and activities are excluded:

- Firms solely engaged in the exchange of physical currency or cheque cashing.
- Software companies that only provide the underlying technology for payments but have no role in handling funds.
- Activities under a banking licence.²
- Corporate entities that only offer non-sales payment services related to operating expenses on their own behalf, such as rent, corporate registry, utilities, or similar services (e.g., accounting service providers).
- Entities identified solely as digital asset service providers (also referred to as Virtual Asset Service Providers (VASPs) or Crypto-Asset Service Providers (CASPs)).³

3. Background

The payments landscape has evolved significantly with the rise of non-bank PSPs, driven by a focus on consumer experience, speed, and cost efficiency. Non-bank PSPs heavily rely on financial institutions (FIs)⁴ for accounts and direct participation in payment market infrastructures, facilitating payments through local payment networks, net settlement, and bundled or bulk transactions, including cross-border transactions. The high levels of intermediation between the originator and the beneficiary increase the challenges for the intermediary FI in monitoring and screening, complicating the FI's ability to understand and manage the financial crime risks associated with non-bank PSP relationships.

The ongoing challenges in finding international alignment in financial crime regulations and licensing requirements in the non-bank PSP sector further hinder FIs' efforts to maintain a common set of financial crime compliance and risk management standards across jurisdictions.

This document aims to set out the controls necessary for FIs to ensure their relationships with non-bank PSPs remain within their risk appetite. It expands on existing Group guidance by detailing common relationship types, associated risks, compliance obligations and risk management expectations for FIs providing services to non-bank PSPs.

² For activity carried out under a banking licence, refer to the [Wolfsberg Group Financial Crime Principles for Correspondent Banking](#).

³ For information on digital assets, refer to [Wolfsberg FAQs on Defining Digital Assets](#) (2024) and [Wolfsberg Guidance on the Provision of Banking Services to Fiat-Backed Stablecoin Issuers](#) (2025).

⁴ While often these are banks, there are increasingly situations where financial institutions that are not categorised as banks provide services to non-bank PSPs. This guidance is intended to serve all FIs that provide services to non-bank PSPs, although specific bank-related scenarios are identified when pertinent.

The principles underlying this guidance emphasise:

- **The risk-based approach:** FIs should apply a risk-based approach to managing financial crime risks associated with non-bank PSP relationships, tailoring due diligence and monitoring to the specific risks presented by different non-bank PSP activities.
- **Payment transparency:** non-bank PSPs, particularly the debtor agent PSP (the originating entity), have a primary obligation to ensure payment messages contain complete and accurate information to comply with FATF Recommendation 16 and local regulations. Intermediary PSPs are crucial in maintaining transparency by controlling and transmitting information without alteration and monitoring for incomplete details, as required by local laws and regulations.
- **Comprehensive risk management:** FIs should have a thorough understanding of a non-bank PSP's business model, customer activities, and the financial crime controls in place to effectively manage associated risks.

4. Non-bank PSP payment activities

The financial crime risk level and typologies associated with a non-bank PSP depend on a broad range of factors, including the business activities and geographic nexus of the activities in which the non-bank PSP engages. It is therefore crucial for FIs to understand the non-bank PSP's business model and the specific financial crime risks that it may present.

Non-bank PSPs' business activities can generally be divided into three categories:

- **Business remittance services:** non-bank PSPs offer financial services and products to businesses for third-party or proprietary payments not related to e-commerce, including domestic and/or cross border payments, cash management, and foreign exchange (FX) solutions. The customers of such non-bank PSPs include corporates, small and medium-sized enterprises (SMEs), and other FIs (including other non-bank PSPs).
- **Person-to-person remittances:** non-bank PSPs provide payment services to individuals domestically or cross-border. Unlike business-related payments, where the nature of business activity may be easier to validate in the public domain, person-to-person payments often lack readily available information about the transacting parties. A distinction should be made between non-bank PSPs providing technology solutions for digital remittances that have no cash elements and those that are primarily cash-focused money transmitters. This includes digital remittances through account transfers, credit card payments, peer-to-peer platforms and e-wallets.⁵

⁵ For the purposes of this document, *e-wallets* refer only to wallets that support fiat-currency transactions and exclude wallets that hold digital assets or enable transactions in digital assets.

Digital remittances may also be enabled in online gaming and social media platforms. Digital assets, such as online tokens, can be purchased and are in some instances transferrable to another person via the gaming or social media platform. If these digital assets can be cashed out, this may be considered a form of digital remittance.

- **Merchant acquiring:** non-bank PSPs enable merchants to accept card and other payments, such as e-wallets relating to the sale of goods and services either online or in physical places of business. Typically, merchant acquiring involves collecting funds from either retail customers, businesses or marketplaces and facilitating settlement to the merchant or supplier. Services that FIs offer typically include collection and settlement accounts.

Other products offered by non-bank PSPs relevant to the three models mentioned above may include:

- Technology-enabled platforms facilitating cash management, payments, and foreign exchange (FX).
- Accounts, often referred to by other terms such as “wallets” or “stored value accounts”.
- Issuing physical or virtual credit cards, debit cards and prepaid cards for businesses to use in payments to suppliers, staff, etc. In cases where a non-bank PSP issues virtual or physical cards, these cards are typically loaded by business customers with funds to be attributed to their respective suppliers or employees, such as for salary payments. In such instances, the card would be used by a third party (i.e., the employee or supplier).

The activities mentioned above are not mutually exclusive as a single non-bank PSP may offer multiple services to its customers through a range of products and solutions. Additionally, the non-bank PSP could act on behalf of other licensed PSPs across all three types of non-bank PSPs’ payment activities. Therefore, it is crucial for the FI to have a thorough understanding of its non-bank PSP customers’ activities and their application of financial crimes compliance controls in each area.

In addition to offering their own services and products, non-bank PSPs may collaborate with traditional FIs (i.e., banks) to offer their customers a range of banking services. This partnership allows non-bank PSPs to leverage the established compliance framework and risk management infrastructure of a traditional FI, enhancing their service offerings and reaching a broader customer base.

Non-bank PSPs may collaborate with traditional FIs through models like:

- **Banking-as-a-Service (BaaS):** non-bank PSPs partner with banks leveraging their technology to extend the FI products such as accounts, lending services, and bank-issued credit/debit cards to a broader audience. In these partnerships, customer onboarding and transactions are typically completed through the non-bank PSP’s platform, instead

of the FI's, and therefore the KYC datapoints and transaction details are collected and recorded by the non-bank PSP. The FI's reliance on the non-bank PSP for record keeping and potentially other aspects of the operations highlights the importance of third-party risk management in these partnerships. The non-bank PSP may also market their offering as BaaS, providing technical infrastructure such as white-labelling solutions to other companies, including FIs and non-bank PSPs, enabling them to embed and offer financial products (like payments or cards) to their customers.

- **Sponsored Account:** non-bank PSPs participate in payment systems by utilising the licence of a sponsoring FI, typically a bank. This arrangement, also known as a Sponsored for-benefit-of (FBO) account,⁶ allows third-party payments to be facilitated through a regulated FI. This setup is particularly advantageous for non-bank PSPs seeking to enter a market or expand their services. However, it requires careful evaluation and management of the risk, as the FI remains ultimately responsible for the activities conducted through its accounts. Specific similar arrangements may exist in other jurisdictions that provide such access to non-bank PSPs.

5. Payment flows and associated risks

In order to evaluate the risk presented by non-bank PSPs effectively, it is critical for FIs to understand the various types of payment flows and the services the non-bank PSP provides through its account with the FI. This includes distinguishing between the type of flows (proprietary, third-party, and bundled payment flows) as each carries distinct financial crime risk implications.

- **Proprietary flows:** a non-bank PSP making payments on its own behalf would be considered proprietary, such as payments for operational activity (e.g., salary payments) or principal-to-principal payments with other FIs. These are often considered lower risk than third-party flows, given that the underlying FI providing the accounts is not exposed to the activity of the non-bank PSP's customers. However, increasingly non-bank PSPs classify "liquidity management" as proprietary activity, when in reality the non-bank PSP anticipates payment disbursements for its customers, which may ultimately facilitate final disbursement to third parties. In such cases the FI may unknowingly be exposed to third party payment risk.
- **Third-party flows:** non-bank PSPs may utilise their account to facilitate payments for their underlying customers, creating third party payment flow exposure for the supporting FI. These flows can involve multiple layers of underlying parties and present varying degrees of financial crime risk. Depending on the type of services an FI provides to a non-bank PSP, the FI may be exposed to the risk associated with the non-bank PSP's

⁶ A Sponsored Account or Sponsored FBO Account is distinct from a broader "FBO account" where an account is held for the benefit of another party.

customer base similar to correspondent activities (in case the FI facilitates non-proprietary flows for the non-bank PSP). Hence, understanding the portfolio of the non-bank PSP's customers is crucial. Depending on the type of flows processed by the FI, and dependent on local regulatory requirements, a safeguarding account may need to be opened to ensure protection of funds.

- **Bundled / Netted / Bulk flows:** bundling refers to the aggregation of multiple payments into a single, often cross-border, payment. The risk varies significantly depending on the type of bundling. For instance, while “one-to-many” bundling scenarios (e.g., salary disbursements) generally pose less significant risk, “many-to-one” (e.g. merchant servicing) or “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) carry higher risk. Many-to-many bundling significantly reduces transparency for an FI providing accounts to a non-bank PSP. This complexity makes screening and monitoring for suspicious activity more difficult, increasing the FI's reliance on the non-bank PSP's controls. Accordingly, the FI should understand and be able to take comfort from the non-bank PSP's risk management framework for its customer base.

To support the management of the risks of the various payment flows associated with non-bank PSPs, FIs should complement traditional due diligence with tailored measures to understand the business model, underlying risk, and compliance framework of each non-bank PSP relationship.

Key risks in non-bank PSP relationships include, but are not limited to:

- **Payment transparency:** non-bank PSPs often route payments through multiple rails, intermediaries, and jurisdictions to deliver faster, lower-cost payments and provide better customer experience. This means the FI providing services to a non-bank PSP may only process one part of the flow rather than the full end-to-end payment chain. As a result, the FI may have limited visibility into the underlying transacting parties and the purpose of the payment, especially in scenarios involving diverse payment methods such as those where card payments are collected from originators in one country and then bundled into an international wire sent to the non-bank PSP in another country for disbursement to beneficiaries via domestic payment systems.
- **Sanctions risk:** reduced visibility over the payment chain also increases the risk that money transfers and payments for underlying goods or services could be connected to sanctioned jurisdictions or restricted parties. This risk is heightened further in scenarios involving bundled payments where the FI may lack visibility into the end-to-end transaction chain. In such cases, the FI depends on the non-bank PSP's sanctions

screening controls, which may vary in effectiveness depending on the non-bank PSP's jurisdiction and regulatory oversight.

- **Money laundering risk:** FIs may have limited visibility into the originator, purpose, and ultimate beneficiaries of funds handled by non-bank PSPs, particularly when multiple payments systems and PSPs are involved in the transaction chain or where payments are bundled. In such scenarios, the FI lacks direct oversight of individual transactions and must depend, to some extent, on the non-bank PSP's monitoring for suspicious activity programme and broader anti-money laundering (AML) controls.
- **Fraud risk:** the payments industry is highly vulnerable to fraud schemes that adversely impact FIs, consumers, merchants and other businesses; this can result in significant harm to consumers and undermine trust in payment channels. Non-bank PSPs often do not have a traditional account relationship with their customers and may lack the long-term behavioural data typically used to detect fraudulent activities or patterns, increasing the risk of fragmented oversight which can weaken fraud detection and escalation, and potentially allow fraud to go undetected or be identified later than it would within a traditional banking relationship.

6. Risk-based due diligence requirements

In order to manage the risks associated with non-bank PSP relationships effectively, the FI should conduct a thorough assessment of the specific non-bank PSP's activities and flow of funds to understand the unique risks the non-bank PSP presents and the mitigating controls they have in place. The following considerations are recommended when completing EDD on non-bank PSPs:

- **Risk-based approach:** different non-bank PSP activities pose varying degrees of risk. Where a non-bank PSP offers products or services across multiple business activities, the most stringent due diligence requirements should apply.
- **Tailored questionnaires:** use tailored questionnaires to facilitate the assessment of specific factors, including the customer's business model, funds flows, payment corridors, and financial crime risk controls.
- **Ongoing due diligence:** in addition to due diligence applied at onboarding, given the innovative nature of non-bank PSPs and the rapid evolution of their business models, commensurate emphasis should be placed on ongoing due diligence, conducted on a risk-based approach. This may include reviews triggered by material events, such as material negative news, ownership changes, financial crime incidents, licensing changes, or the introduction of new flows or intermediaries.

By taking these steps, FIs can better manage the risks associated with non-bank PSP relationships and monitor the non-bank PSP's activity against their own established risk appetite.

Key elements to consider when applying a risk-based approach and conducting EDD on non-bank PSP relationships include:

Business model considerations

FIs should clearly understand their non-bank PSP customers' business models to assess risks appropriately and maintain oversight throughout the relationship. Any significant changes to the non-bank PSP's business model or the nature of their relationship with the FI should trigger a risk-based reassessment. Key considerations for the non-bank PSP include:

- **Types of services:** types of services offered by the non-bank PSP should be considered, including whether they support business payments, digital person-to-person remittances or merchant acquiring, as different service types present varying financial crime risk profiles.
- **Cross-border transactions:** cross-border payments are higher risk from a financial crime perspective as compared to domestic payments, given the potential involvement of parties in different (and under potentially less stringent) regulatory regimes, complex transactions involving multiple parties, limitations in payment transparency, potential exposure to sanctioned entities, and elevated risk of fraud, corruption and other financial crime risks.
- **Funding methods:** high-risk funding methods (e.g. anonymous or hard to trace sources like cash, money orders, prepaid cards) may hinder the ability to trace the origin of funds and identify suspicious activity
- **Non-resident customers:** products or services offered to non-resident customers, particularly those located in high-risk jurisdictions, present elevated risks due to challenges in understanding cross-border and local financial crime risks and licensing requirements.
- **Partner networks:** non-bank PSPs partnering with other PSPs or third parties, for the disbursement of funds to the final beneficiary or e-commerce collections, extends their geographic reach without requiring multiple licences or establishing local branches. The risks associated can impact the overall risk profile of the non-bank PSP. This includes identifying nested relationships and assessing and understanding the division of functional AML/sanctions responsibilities between the non-bank PSP and the partner. Consideration should also be given to how the non-bank PSP maintains oversight of the partner, as well as the level of transparency and due diligence applied across the payment chain.

- **Agents:** non-bank PSPs engaging agents to deliver payment services and products on their behalf. Key considerations for potential risks include the non-bank PSP's ability to maintain effective oversight and control over the agent's activities, particularly where agents perform onboarding, KYC or other financial crime controls. The nature of the principal-agent relationship should be clearly defined, and the principal PSP must ensure that appropriate governance, monitoring, and accountability mechanisms are in place. The non-bank PSP must also assess whether the agent requires registration or licences based on local regulations.

Licensing regime

FIs should document the non-bank PSP's licensing status, understanding that some payment services may not require licensing or AML registration. It is crucial to have a general understanding that the licensing aligns with the non-bank PSP's business model, particularly for the activities supported by the FI. Specific permissions, passporting, and the need for local licences in each jurisdiction of operation should be considered.

Jurisdictional considerations

- **Operating jurisdiction:** the quality of the financial crime compliance regime and regulatory supervision, where the non-bank PSP operates. This includes evaluating the scope and enforcement of local financial crime compliance requirements, as well as the PSP's licensing status and any passporting arrangements that allow cross-border operations. Where relevant, consider the jurisdiction of the PSP's parent entity, particularly if strategic or operational decisions are influenced at the group level and/or if all subsidiaries adhere to group-issued policies and procedures.
- **Payment corridors:** the risks of the jurisdictions involved in payment flows, particularly exposure to high-risk jurisdictions.
- **Underlying customer jurisdictions:** the geographical risk of the non-bank PSP's customer base, such as merchant locations for the merchant acquiring non-bank PSPs. Consideration should also be given to the non-bank PSP sanctions controls, such as how they assess indirect sanctions exposure including the origin/destination of goods.
- **Nested/ downstream activity:** for the non-bank PSPs offering nested/downstream activities, the jurisdictions and the quality of the financial crime regulatory supervision where the underlying entities are based.

Customer-type risk appetite

Each non-bank PSP may have a unique risk appetite when it comes to the type of customers being targeted and onboarded. The FI should assess whether the non-bank PSP has relevant and robust controls to manage the risk they may face through their customer types. The non-

bank PSP's risk appetite should align with that of the FI, and any discrepancies should be resolved by agreeing which payment flows to support.

Non-bank PSP financial crime risk management controls

To understand whether the non-bank PSP can effectively manage the financial crime risks to their business, a comprehensive assessment of the non-bank PSP's financial crime controls is crucial. Areas to evaluate may include:

- **Compliance resources:** assess the qualifications and experience of senior compliance staff, such as the money laundering reporting officer (MLRO) and chief compliance officer (CCO), and outsourced compliance support. Ensure compliance staffing levels are, and remain, commensurate with the PSP's business strategy and the regulatory framework to which it is subject.
- **Governance:** evaluate the framework regarding senior management oversight, compliance escalations, governance committees, and the scalability of the non-bank PSP's compliance programme with business growth.
- **Customer due diligence:** review the non-bank PSP's processes for customer identification and verification, including beneficial ownership, client risk ratings, and periodic reviews. Confirm when EDD for high-risk customers is triggered and how it is tailored to the specific risk profile and implemented in practice.
- **Third-party due diligence:** assess the non-bank PSP's third-party risk management processes for identifying and mitigating financial crime risks of its agents, distributors, partners, vendors, and other third parties. Third-party due diligence controls should also be considered when overlaid with the non-bank PSP's anti-bribery and corruption (AB&C) controls.
- **Product controls:** determine whether the non-bank PSP conducts new and ongoing product risk assessments and due diligence, e.g., utilising transaction caps and limits where appropriate and monitoring customer usage of products.
- **IP monitoring and blocking:** determine if the non-bank PSP utilises geolocation monitoring tools, such as internet protocol (IP) address screening, to detect and block attempts to access their services when originating from sanctioned jurisdictions.
- **Name screening:** evaluate processes for screening customers against sanctions, politically exposed persons (PEPs), and internal watchlists, as well as for financial crime adverse media. This analysis should include the tools or technology used, screening frequency, source of the lists being screened against, identifying and screening connected parties and escalation process.

- **Payment sanctions screening:** assess whether screening for transactions is automated or manual, completed in real time, the tool/vendor used, the quality of screening criteria (e.g., fuzzy logic, payment fields), data elements screening (particularly any free text fields) and the sanctions lists being searched.
- **Monitoring for suspicious activity:** consider whether monitoring is manual or automated, the number of alerts and sufficient resources/controls for any potential backlogs, real time or post transaction monitoring, nature of scenarios, escalation procedures, and resource allocation for reviews.
- **Use of machine learning (ML) and artificial intelligence (AI):** understand how the non-bank PSP uses ML and/or AI as part of their controls and processes (e.g., AML, fraud, sanctions alert creation and/ or investigations), including any independent assessment of their ML and AI use cases to ensure oversight, sufficient expertise, explainability and effectiveness.
- **Management information:** understand metrics and reporting for the overall financial crime compliance and risk management framework for the non-bank PSP. This may include any existing or recent backlogs in transaction monitoring, KYC renewal or other areas of operations, as well as outstanding enhancements as a result of independent audit, examinations or internal risk assessment. FIs should understand the root cause of these issues and confirm the non-bank PSP has a remediation plan to address current matters and reduce the likelihood of recurrence.
- **Payment transparency:** understand the controls for completeness of the transaction details and compliance with FATF Recommendation 16 rules and other applicable regulatory requirements,⁷ dependent on jurisdictional requirements and payment method (e.g., Travel Rule), and the Group's guidance on this subject.
- **Fraud monitoring:** understand the approach to fraud detection including use of IP/device tracking, and identification of fraudulent documents, as well as the speed of response. This may include evaluating the fraud alert, the frequency of fraud risk assessments, and whether the non-bank PSP monitors fraud risk metrics.
- **SAR filing:** review the non-bank PSP's investigation and SAR filing processes, including their understanding of SAR filing obligations in applicable jurisdictions as well as the existence and oversight of internal reporting metrics.
- **Audit framework:** understand the scope and frequency of internal and/or external audits relating to the non-bank PSP's financial crime risk management programme. Where external auditors are used, FIs may consider the reputation of the auditing firm.

⁷ For additional information on payment transparency, refer to the [Wolfsberg Group - Guidance on Payment Transparency, Roles and Responsibilities](#).

The FI may consider any material findings of internal or external independent audits, and regulatory exams relating to financial crime, including remediation efforts.

- **Anti-bribery and corruption (AB&C):** confirm policies and controls to prevent bribery and corruption risks.
- **Training:** assess the frequency, coverage and monitoring of financial crime-related training for staff.
- **Enterprise risk assessment:** ensure the non-bank PSP regularly assesses financial crime risks and the effectiveness of controls.

Additional considerations

- **Length of operations and demonstrated compliance/risk management history:** FIs may use public domain sources to assess the non-bank PSP's operational history and management of financial crime risk (for example, past enforcement actions). Assessment of a newly established non-bank PSP may include additional bespoke due diligence, such as more frequent reviews during its growth phase or obtaining information regarding external audit reports on its control framework.
- **Growth strategy:** non-bank PSPs often innovate rapidly, launching new products and entering new markets; therefore, FIs should consider the non-bank PSP's growth strategy, including planned activities and geographies, and their ability to scale compliance and financial crime controls.
- **Account activity reviews:** FIs should review the non-bank PSP's account activity to detect unexpected changes, such as shifts in payment volumes, new payment corridors, patterns of any potential sanctions' violations or concerns of the emergence of high-risk underlying customers or jurisdictions. This differs from traditional monitoring for suspicious activity, focusing instead on identifying broader unexpected changes in customer behaviour or product usage, or elevated risks such as unexpected nesting or reduced payment transparency. Findings from account activity reviews should inform the periodic EDD reviews.

Based on the outcome of the above risk and controls assessments, FIs should determine whether to onboard/maintain the non-bank PSP relationship or decline/exit, consistent with their risk appetite and the specific payment flows supported. Where risks cannot be sufficiently mitigated—particularly given reduced end-to-end visibility—FIs should consider an appropriate risk-control strategy to manage the exposures they face.

7. Conclusion

The ability of FIs and non-bank PSPs to maintain mutually productive commercial relationships, founded on sound risk management principles, is key for meeting

global ambitions of cheaper, faster, more accessible, and safer payments. An FI's decision to provide banking services to non-bank PSPs is not a simple one, and if not managed appropriately under a risk-based approach, it may risk its participation in various payment market infrastructure schemes and its relationships with home and host country regulators. As many authorities continue to maintain heightened expectations for FIs as "gatekeepers" of the international financial system, these challenges will persist in the absence of a level playing field. High compliance and risk management costs, driven by a combination of complex business models and inconsistent licensing and associated supervisory regimes, often limit the commercial appeal of engaging in the provision of third-party payments for non-bank PSPs, which may not always be subject to the same rules for the same activities and risks as FIs.

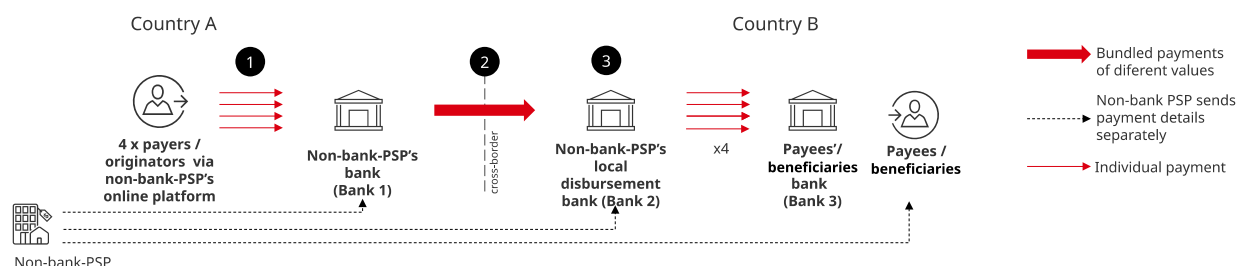
With the release of this guidance, which is intended to complement existing Wolfsberg guidance on correspondent banking and payment transparency standards, the Wolfsberg Group aims to establish a risk-based, reasonable control framework for the provision of payment services to non-bank PSPs, in order to better facilitate and inform an FI's decision-making better, both in engaging in such activity and in managing such relationships within its own risk appetite.

Appendix

The following pages include diagrams of third-party payment flows for non-bank PSPs. The diagrams serve to highlight the complexity of the non-bank PSPs' business models and cover a range of scenarios, with varying levels of intermediation and modes of payment. The diagrams are non-exhaustive examples of the non-bank PSPs' payment flows. Furthermore, the third-party payment flows illustrated in the diagrams highlight potential challenges for FIs providing banking services to non-bank PSPs, including (but not limited to) limited payment transparency and the involvement of a wide range of payment actors subject to varying levels of regulatory supervision.

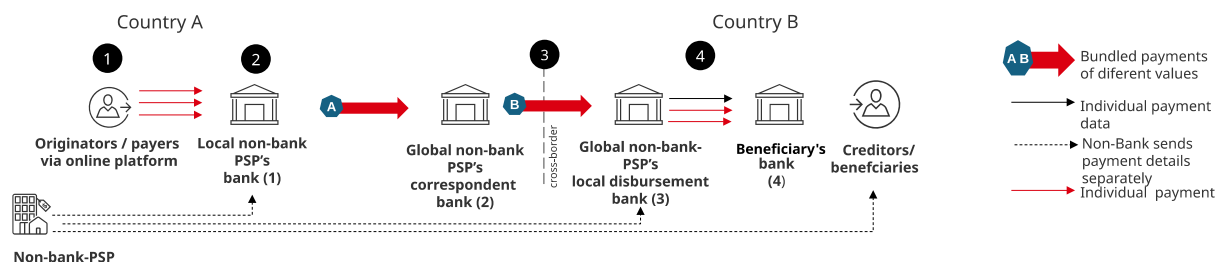
1.1 Example of a simple non-bank PSP funds flow, without additional nesting or partnerships, demonstrating person-to-person digital payments:

In this example the non-bank PSP maintains a relationship with a correspondent which has branches in Country A and Country B.



1. Funds are sent by the non-bank PSP (1) customers – the Payers / Originators in the diagram – to the non-bank PSP's bank, which is banked by Bank 1.
2. Bank 1 sends a bundled transfer to Bank 2 in Country B, which holds an account for the non-bank PSP in Country B.
3. Following receipt of the instructions from the Originating non-bank PSP, Bank 2 makes the payment to the Payee/Beneficiaries into their bank accounts at Bank 3.

1.2 Example of a nested non-bank PSP fund flow:



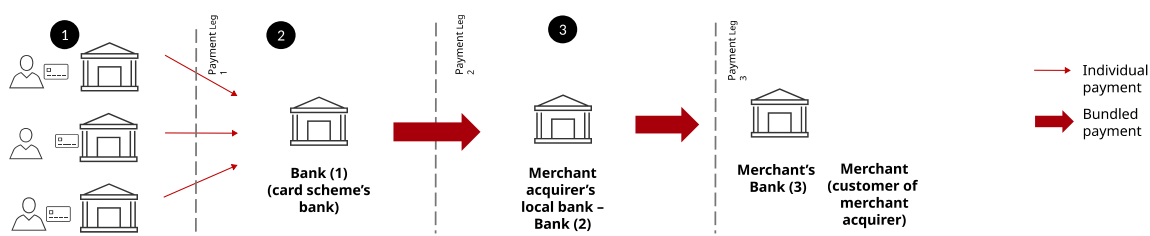
The global non-bank PSP (i.e., customer of Bank 2) provides services to local small banks and/or non-bank PSPs, which use the global non-bank PSP's network to make payments on behalf of their underlying customers. The common reasons for using global non-bank PSPs may be their more favourable foreign exchange rates, their ability to make payments to a broader range of jurisdictions or delivering funds to the beneficiaries using a wider range of payment options.

This example assumes a cross-border remittance where a local non-bank PSP is customer of a global non-bank PSP and uses global non-bank PSP for payments from the originator in Country A to the beneficiary in Country B. This flow is considered nested for Bank 2, given the global non-bank PSP is facilitating payment for their customer's underlying customer.

- 1. Initiation by the Originator/Payer:** the Originator/Payer, who is a customer of the local non-bank PSP, initiates a remittance transaction online or via an App. For the funds, the Originator/Payer can either transfer funds from their own bank account to the local non-bank PSP's bank account or use funds already available in Originator/Payer's wallet held with the local non-bank PSP.
- 2. Payment from the local non-bank PSP to the global non-bank PSP:** the local non-bank PSP aggregates all remittance requests destined to Country B and sends a bundled payment from its bank account to the global non-bank PSP's bank account. Additionally, the local non-bank PSP provides detailed instructions to the global non-bank PSP for each beneficiary who is to receive a payment.
- 3. Cross-border transfer:** the global non-bank PSP transfers a bundled payment from its bank account in Country A to Country B. The global non-bank PSP may have its own bank accounts in both Country A and B or use its affiliates in Country B to facilitate the payment to the beneficiaries.

4. **Final payments to beneficiaries:** the global non-bank PSP disburses the funds from its bank account to each beneficiary's bank account, following the instructions received from the local non-bank PSP. The beneficiary's bank would then credit the beneficiary.

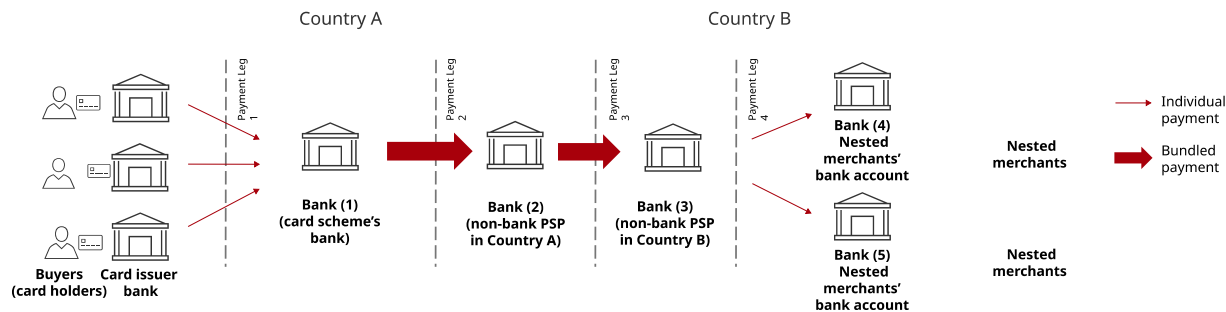
1.3 Example of a non-bank PSP conducting merchant acquiring – settling card payments for goods and services including e-commerce:



1. Buyers pay with a card in a shop or on-line. 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, Bank (1). Card issuers are repaid by the card holder separately.
2. Bank (1) pays all the money due in a bundled payment to Bank (2), the merchants acquirer's bank.
3. The merchant acquirer's bank, Bank (2), makes payments to the individual merchant's bank (3) as per agreement (monthly, weekly, daily).

Note: the non-bank PSP is the merchant acquirer

1.4 Example of a non-bank PSP conducting merchant acquiring – settling card payments for goods and services, e-commerce, with more than one non-bank PSP involved (i.e., nesting):



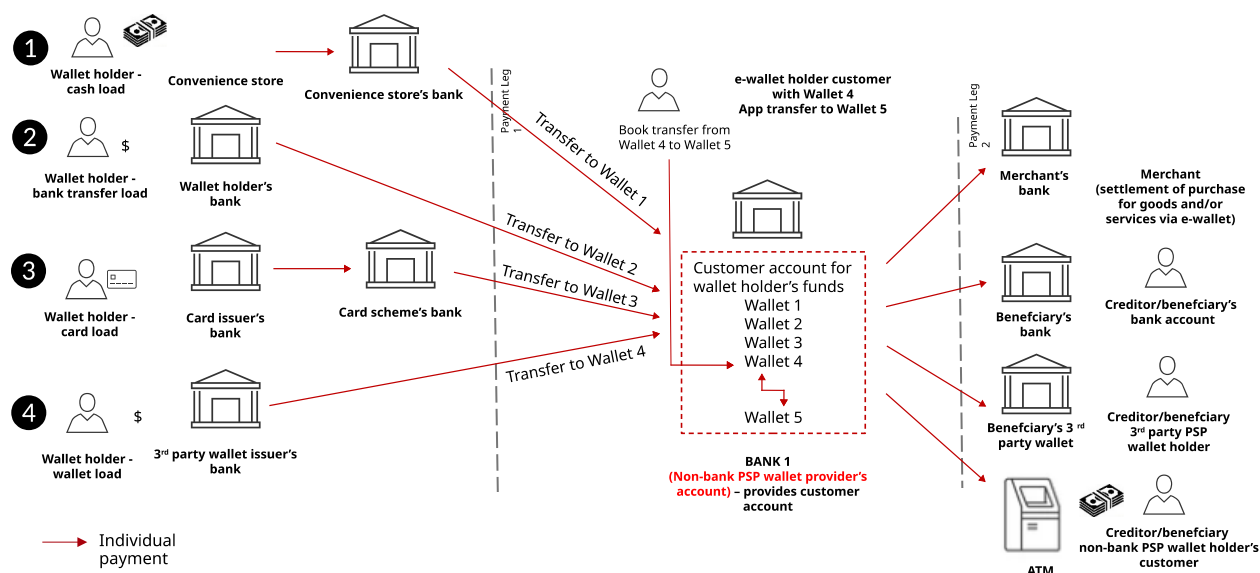
Buyers in Country A make a purchase online from merchants in Country B.

1. The card settlement process starts with the collection from the card issuers who use their national net settlement scheme to transfer, in bulk, of all their customers transactions to card scheme's bank account at Bank (1). Card issuers are repaid by the card holder's bank account in a separate transaction.
2. The card scheme transfers from their bank account at Bank (1) the settlement of all funds due to the merchants in Country B to the non-bank PSP bank in Country A at Bank (2).
3. As the non-bank PSP in Country A does not have presence or a group company in Country B, they use another non-Bank-PSP to make the disbursements to the merchants in Country B. This is considered nesting, because non-bank PSP in Country A has not onboarded or undertaken the due diligence on merchants in Country B. Bank (2) makes a cross-border transfer to Bank (3) in Country B to the non-Bank PSP's account.
4. The final payment leg is the payment from the non-bank-PSP's Bank (3) in Country B to the various nested merchants who have accounts at Bank (4) and Bank (5).

Note: This is the basic payment flow for the card settlement transactions. It does not represent the end-to-end card scheme payment cycle.

1.5 Example of a complex business model using e-wallets:

In this example, the FI's customer is a non-bank PSP that issues stored value payment instruments/ e-wallets (referenced going forward as a "non-bank PSP wallet provider"). The wallets can be used to make person-to-person digital payments or to purchase goods and services, either domestically or cross-border. The non-bank PSP wallet provider may also issue a card sponsored by a card scheme that is linked to the non-bank PSP wallet provider's customer's wallet, enabling cash to be withdrawn via ATMs worldwide. To enable these services to its customers, the non-bank PSP wallet provider establishes a customer account⁸ at Bank (1) to hold its customers' funds (i.e., the wallet holders' funds). Within that customer account, the non-bank PSP wallet provider has a ledger tracking the transactions applied to each wallet.



Individual or bundled payment

The e-wallets can be loaded four ways with cash via convenience stores, by bank transfer, by card payment and by transfers from another third-party e-wallet. Each payment flow can give varying degrees of payment visibility.

Loading e-wallets

1. Credits from a chain of convenience stores or acting as an agent for the non-bank PSP wallet provider or partnering with other PSPs, enabling the non-bank PSP wallet provider's wallet holders to load their e-wallets with cash.

⁸ In some regions this may be required to be a "safeguarding" account per regulation.

2. Credits from the underlying non-bank PSP wallet provider customers, loading their e-wallets from their local bank accounts.
3. Credits to the customer account from the non-bank PSP wallet provider's customers loading their e-wallets via card transactions.
4. Credits from the non-bank PSP wallet provider's customers from another PSP wallet provider.

Outgoing payments from the e-wallets:

1. Debit from the non-bank PSP's account to the merchant represents a "cash out" of the merchant's funds from its e-wallet at the non-bank PSP wallet provider to an account that the merchant holds at another bank/FI/PSP. As the "cash out" is a separate transaction, the details of the underlying sales would not be visible to Bank (1) that provides the non-bank PSP wallet provider's customer account.
2. Debit remittance from the customer account to the overseas or domestic bank account of a beneficiary.
3. E-wallet to an overseas or domestic third-party e-wallet holder; an agreement must be in place with the third-party e-wallet holder to accept the e-wallet. The non-bank PSP wallet holder, the underlying customer, will have an option to send via this method on their application.
4. E-wallet to overseas or domestic ATM cash withdrawal. The withdrawal can be either via a physical card, or specialised ATMs which can allow cardless withdrawals by generating a QR via a mobile app.