ENHANCING CROSS-BORDER PAYMENTS: FAST PAYMENT SYSTEM INTERLINKING

Cross-border Payments Interoperability and Extension (PIE) task force:
Task Team 2

February 2026

This report was prepared by a group of PIE task force members (task team 2), with additional inputs and comments from other parties. The views expressed in this report do not necessarily reflect those of the Bank for International Settlements (BIS), the BIS Committee on Payments and Market Infrastructures (CPMI), its member central banks or of the whole PIE task force and its members.

PIE task force reports are written by industry stakeholders who are members of the PIE task force, sometimes in cooperation with other experts. The views expressed in them are those of the authors and not the views of the Bank for International Settlements (BIS), the BIS Committee on Payments and Market Infrastructures (CPMI) or its member central banks. The authors bear sole responsibility for the accuracy of the information as of Q4 2024 and the correctness of its citations in this report.

The terms "country", "jurisdiction" and "economy" used in this publication also cover territorial entities that are not states as understood by international law and practice but for which data are separately and independently maintained. The designations used and the presentation of material in this publication do not imply the expression of any opinion on the part of the BIS concerning the legal status of any country, area or territory or of its authorities, or concerning the delimitation of its frontiers or boundaries. Names of countries or other territorial entities are used in a short form which is not necessarily their official name.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

For the purpose of this report, fast payment systems (FPS) are defined as a set of rules, practices, procedures, standards, services, applications and infrastructure needed to provide and operate a specific payment instrument which is settled instantaneously between payment service providers (PSPs). FPS *interlinking* arrangements allow bank and non-bank PSPs to transact with each other across different jurisdictions, with the aim of shortening transaction chains, reducing costs, and increasing transparency and speed of payments, without requiring participation in the same system or using intermediaries.

The G20 has identified the interlinking of FPS as a priority action within its Roadmap to enhance cross-border payments. Yet, establishing an FPS interlinking arrangement requires more than technical connections. Several challenges, which are partly outside the sphere of influence of the FPS owners and operators, need to be addressed for the establishment of cross-border payment links. These challenges include:

- A **lack of universal standards** and an inconsistent adoption of the global payment messaging standard ISO 20022, leading to difficulties in establishing interoperability.
- **Differences in operational frameworks and scheme rules** negatively impact end-to-end solutions.
- The **lack of multicurrency** support and cross-currency conversion in most FPS introduces costs and frictions to deal with cross-border payments.
- Ambiguity and inconsistency in **governance and oversight** leads to uncertainties over the delineation of responsibilities between the scheme owner, technical operator and PSP, impacting contractual obligations and legal certainty.
- A **lack of a common regulatory and compliance approach,** specifically in the areas of sanctions compliance, data protection and regulatory reporting between countries represents another barrier to the efficiency and equivalence of interlinked FPS.
- The need for **multiple stakeholders** to interact across jurisdictions can add friction and create challenges in meeting timeframes required for an end-to-end real-time flow.

These challenges are explored further in section 3 of this report. Taken together, these factors tend to increase the costs of FPS interlinking. As a result, links might not be established at all or links may be less effective, resulting in payment delays, high rejection rates, high fees, and increased fraud risks. Ultimately, the challenges could also lead to poor customer experiences.

The opportunity to leverage FPS for cross-border use is sizeable: a stocktake conducted in Q4 2024 for this report, covering 54 FPS (representing around 60% of the total estimated in operation), suggests that approximately half of the FPS surveyed have the potential to support cross-border payments. This is explored further in section 4 of the report.

Task Team 2, composed of payments industry representatives of the Payments Interoperability and Extension (PIE) task force convened by the CPMI, along with other experts, has developed considerations to address the challenges of interlinking of FPS for cross-border payments. Drawing on industry expertise and good practices of various approaches leveraging FPS for cross-border use, this report suggests possible steps for public bodies and the private sector, including FPS owners and operators, to enhance cross-border payments through the interlinking of FPS.

Task Team 2 believes that the suggested steps are important to meet the G20 Roadmap objectives and deliver widespread benefits for citizens and economies worldwide. While the suggested next steps are ambitions, Task Team 2 believes that a less aspiring approach would lack clarity of vision, pace, and direction. The steps are addressed to FPS owners, operators, PSPs as well as public bodies with the recognition that taking them forward will require collaboration and coordination. Specifically, detailed work will be required for a pragmatic, sequenced, and proportionate approach considering

competing priorities, assessing for unintended consequences, and subjecting proposals to analysis and consultation. The considerations and next steps suggested by Task Team 2 are summarised in the following ten points.

1. Enable all FPS domestic schemes and systems rules to send and receive cross-border payments.

- FPS operators should evaluate domestic schemes to ensure they can support the functionality and processes needed for cross-border payments. While sending cross-border payment is optional, domestic schemes should be able to receive cross-border payments.
- FPS operators, when upgrading and renewing domestic FPS capabilities and processes, should prioritise enabling FPS interlinking for cross-border use. Ideally, this process to send and receive cross-border transactions should not require renewed onboarding of the existing FPS scheme participants.

2. Foster FPS interoperability through continued alignment to common standards.

- FPS operators should contribute to and align with technical standards and ongoing efforts to achieve interoperability of messaging standards, processes, technologies, and infrastructure.
- FPS operators, in collaboration with PSPs, should support the consistent implementation of ISO 20022, accompanied by agreed-upon market practice guidelines, to foster true interoperability.

3. Provide reciprocity (similar service propositions on both sides of a cross-border transaction) at a reasonable cost.

- PSPs should support a consistent user experience on both sides of a cross-border transaction, so that end users are benefitting from similar service propositions for cross-border payments.
- PSPs and FPS operators should establish reciprocity arrangements with other PSPs and FPS operators. They should take a phased approach to achieving reciprocity arrangements that reflect market demand and desired end user outcomes while ensuring that reciprocity of services is provided at a reasonable cost by FPS operators to achieve commercial viability of interlinking arrangements.

4. Prioritise harmonisation of anti-money laundering (AML) checks and sanctions screening while preserving their highest effectiveness.

- The public sector should prioritise the harmonisation of AML and all sanctions screening requirements to enable the private sector to screen more efficiently, thereby reducing unnecessary frictions and costs in processing cross-border payments.
- Both the public and private sectors should resume work to allow further improving both the efficiency and effectiveness of AML and sanctions screening. This includes assessing technologies to support automation, evaluating the applicability and harmonisation of international best practices, and recognising the crucial role of the Financial Action Task Force (FATF) in engaging with industry practitioners.

5. Increase access for non-bank PSPs to FPS based on the principle of "same activity, same risk, same regulation."

- FPS operators should widen the options for non-bank PSPs to participate in FPS through direct or indirect access in alignment with central banks and regulatory authorities' frameworks. Non-bank PSPs (such as regulated institutions like e-money providers) can help diversify use cases including addressing gaps in customer access, and further financial inclusion goals.
- Non-bank PSPs that align with the Wolfsberg Group's payment transparency recommendations,[1] could get easier direct access to real-time gross settlement (RTGS) systems. This could open up market choice for access and reduce non-bank PSPs' overhead cost of indirect participation, furthering their ability to drive innovation and competition.
- Public authorities should consider regulating on the principle of "same activity, same risk, same regulation" – with ideally the same regulatory bodies providing and coordinating consistent and proportionate supervision of both bank and non-bank PSPs with direct access.

6. Adjust fast payment transaction value limits to support expanded use cases and higher-value payments.

- FPS operators should set transaction value limits in a manner that accommodates diverse use cases, ensuring the benefits of interlinked FPS can be fully realised. They should also address risks by leveraging advanced fraud prevention tools, enabling 24/7 liquidity availability in coordination with liquidity providers, and evaluating appropriate settlement models.
- Sending PSPs should be able to decide on their transaction value limits based on their own risk appetite and business models.

7. Address the e-commerce use case.

- FPS operators and PSPs should establish a clearly defined and cohesive FPS interlinking approach for cross-border e-commerce use cases. This will help increase transaction volumes, enhance the economic benefits of implementing interlinking arrangements, and reduce unit costs.
- To support e-commerce use cases, FPS operators and PSPs should conduct further studies on various e-commerce use cases, with the aim of achieving worldwide adoption of best practices and related requirements.

8. Support proxies and aliases such as mobile phone numbers, and wallets to increase customer access.

- FPS operators should enable the adoption of proxies and aliases, such as mobile phone numbers, to also facilitate cross-border transactions (at least when available for domestic use). This would reduce friction, improve the customer experience, and potentially reduce costs by reducing the number of errors and implied disputes in transaction. Existing domestic proxy/alias resolution services will need to be enabled to support cross-border use. This will likely require public sector support to address the potential challenges of cross-border data

[1] Wolfsberg Group (2024): Payment Transparency Roles and Responsibilities

sharing for cross-border proxy resolution purposes, while solutions such as privacy-enhancing technologies could be explored to mitigate concerns.

- Payment schemes should consider the implementation of domestic confirmation of payee services that can support cross-border pre-validation.
- FPS operators should increase consumer access including by wallet providers, also aiming to foster financial inclusion.

9. Facilitate cross-border information exchange to combat fraud.

- Industry participants should actively share current domestic fraud mitigation practices with other stakeholders. These practices include the confirmation of the identity of the beneficiary (as required by applicable screening standards) and establishing recovery paths between PSPs. This can help to build a collaborative and efficient framework for cross-border payment fraud mitigation. Efficient operational information exchange will require institutions to work together on common fraud data taxonomies.
- PIE Task Team 2 considers that the broader ecosystem involved in FPS interlinking, including telecommunication companies, social media platforms and public authorities, has a shared responsibility for preventing fraud.[2]

10. Prioritise increasing alignment of governance and oversight frameworks for FPS interlinking arrangements.

- Public authorities and PSPs, in coordination with FPS operators, should seek alignment on underlying governance, commercial and technical models of interlinking arrangements across jurisdictions to incentivise their adoption, scalability, and viability.
- Public authorities should ensure that the roles and responsibilities of overseers, scheme owners, technical operators, and FPS participants are appropriately defined to ensure efficient and effective control of operations.

[2] See the report by Task Team 2 on addressing fraud in cross-border payments that sets out the task team's considerations to mitigate fast payments fraud risk.

1. INTRODUCTION

Enhancing cross-border payments' speed and transparency, while increasing access to cross-border payment services, reducing their costs and maintaining their safety, are the key objectives of the G20 Roadmap for cross-border payments.

Since the G20 leaders endorsed the Roadmap for enhancing cross-border payments in 2020, much has been accomplished in laying the foundations through the necessary stock takes and analysis. As the programme has turned to implementation, the Bank for International Settlements' (BIS) Committee on Payments and Market Infrastructures (CPMI) and the Financial Stability Board (FSB) have organised the work around three priority themes: (i) interoperability and extension of payment systems, (ii) data exchange and messaging standards, and (iii) legal, regulatory and supervisory frameworks.

The CPMI-convened cross-border payments interoperability and extension (PIE) task force's primarily focuses on strengthening private sector participation in pursuing the key objectives of the G20 cross-border payments programme. As of 2024, the PIE task force has more than 30 representatives from industry associations, financial infrastructures and PSPs, covering a wide range of business models and geographic areas.

In 2023 and 2024 the PIE task force focused on improving access to payment systems and currencies, extending payment system operating hours, promoting the use of fast payments for cross-border transactions and fostering the harmonised implementation of messaging standards (such as ISO 20022 and application programming interfaces (API) standards and requirements).

This report on FPS interlinking has been drafted by PIE task force Task Team 2 and focuses on interlinking of domestic and regional FPS for the provision of cross-border payments. Task Team 2 members contributed their expertise on, and experience with domestic, regional and interlinked FPS, covering both retail and wholesale payment operations. The perspectives of bank and non-bank PSPs, card schemes, and financial infrastructures have been included in the report.

The report sets out industry considerations of the opportunities and challenges of FPS interlinking. It is based on a detailed stocktake of 54 FPS (representing 60% of the estimated current FPS in operation), carried out by Task Team 2, to lay the foundation of an evidence-based analysis. The inventory resulting from the stocktake provides a source for industry intelligence and can form the basis for initiating collaboration between schemes. The report also includes case studies of FPS interlinking arrangements to identify best practices and concludes with suggested next steps for public bodies and the private sector to take forward activities that promote FPS interlinking.

2. FPS INTERLINKING ENABLING CROSS-BORDER PAYMENTS

An FPS is a payment system that operates 24 hours, seven days a week, 365 days a year (24/7/365). It is characterised by the transmission of the payment message and the availability of funds to the payee within few seconds, which is often referred to as "real time," "near-real time" or "instantaneous" settlement.

There are a number of key roles in an FPS: an FPS operator, responsible for managing the legal and commercial relations between the different parties; a technical operator, mandated by the FPS operator to ensure the system runs smoothly from a technical perspective, and a scheme owner, which may or may not be different from the FPS operator, and is responsible for setting the rules of exchange for a given payment means.

FPS is a volume-driven business, supporting many retail, consumer, and business use cases. FPS are distinct from High-Value Payment Systems (HVPS), which are typically operated by central banks to handle high-value, relatively low-volume wholesale payments for corporate and treasury functions.

Payment system *interlinking* arrangements allow bank and non-bank PSPs to transact with each other across different jurisdictions, with the aim of shortening transaction chains, reducing costs, and increasing transparency and speed of payments, without requiring participation in the same system or using intermediaries.

FPS interlinking arrangements across borders are supported by contractual agreements, technical links and standards and operating procedures between two or more FPS from different jurisdictions. They allow the PSPs participating in an FPS to send and receive fast payments safely and efficiently to PSPs in another jurisdiction's FPS without being a participant in that FPS or opening settlement accounts with correspondent banks.[3]

The G20 has identified the interlinking of FPS as a priority action to help achieve its Roadmap objectives to enhance cross-border payments. Interest in the benefits of FPS – speed, 24/7/365 availability and access to a growing number of end users – has led to considerations for connecting or 'interlinking' multiple domestic FPS operations to support cross-border payments.

Unsurprisingly, most FPS around the world support only their local currencies as their focus is on domestic payments. However, some countries and regions have implemented multi-currency systems facilitating transactions in several currencies. It is acknowledged, however, that the feasibility of supporting multiple currencies in a domestic system depends on the availability of high-volume corridors to support the return on such investment.

For both single-currency and multicurrency FPS, interoperability with other FPS processing other currencies would help to enhance cross-border payments in terms of speed, cost and transparency. The characteristics of domestic FPS are set out in Table 1, the process of cross-border payments processing by FPS is depicted in Figure 7 (Annex A).

Table 1: FPS characteristics

Instant and always on 24/7/365 capability	Payments may be processed instantly as real-time payments, in near-real time or, depending on the scheme rules, usually with a response time of no more than a few seconds. Within this timeframe, the receiving institution will indicate that the payment has been accepted, conditionally accepted or rejected, to be able to make funds available to the payee.

[3] CPMI (2024): *Linking fast payment systems across borders: governance and oversight – Final report*, October.

	Sometimes payment transactions are flagged for further analysis (for example, due to potential sanction hits) before being credited to the beneficiary. However, the vast majority of payments are processed and credited within seconds or minutes. FPS primarily offer 24/7/365 functionality with beneficiary accounts able to send and receive funds at any time and instantly. The funds are typically irrevocable – once transferred within specified time limits, they cannot be returned in the same transaction.
Payment types and limits	FPS typically support domestic retail payment types such as single immediate payments or regular, forward-dated payments. Additional payment types include aggregated bulk payment files directly submitted by corporates or by service bureaus on their behalf. Payment transaction limits vary based on jurisdiction regulation, governance and market practices.
Access to and membership of FPS	Each FPS owner will have their own scheme rules, that the FPS operator is required to comply with, and that apply to operators and PSPs with direct FPS access, setting out technical requirements, scheme obligations, operational rules and oversight mechanisms. In certain jurisdictions the FPS owner might also be the scheme operator. FPS participants, with direct FPS access, tend to be credit institutions with a settlement account at the respective central bank. FPS operate primarily for interbank transactions but are increasingly opening access to non-bank money service businesses (MSBs), such as e-money institutions, wallets and remittance providers, although license requirements and authorisations may vary across jurisdictions.
Clearing, settlement and funding	FPS can settle transaction individually or offer automated clearing with deferred inter-PSP settlement of net amounts. In both cases, end users are typically credited irrevocably within seconds or minutes, allowing the beneficiary to use the funds as they wish, without any third party having the ability to recall them. An FPS may use a variety of settlement and funding models (eg pre-funding, multilateral deferred net settlement), including dynamic management of participant liquidity, depending upon what is available during the business hours of the RTGS system and the regulatory regime.

Source: PIE Task Team 2.

3. CHALLENGES TO INTERLINKING FPS FOR CROSS-BORDER PAYMENTS

Designing, implementing and operating an FPS is complex, and interlinking FPS even more so. Establishing an FPS interlinking arrangement requires more than the commitment of the FPS owners to technically connect the systems. Often, challenges outside the sphere of influence of the FPS owners need to be addressed before cross-border FPS links can be established. Differences in technical, legal and regulatory frameworks, even if well understood, may be challenging to align amongst participating jurisdictions.

Challenges to interlinking FPS include:

- **Lack of universal standards and interoperability.** Interlinking requires standardised formats for messaging, settlement, and compliance. While ISO 20022 is emerging as a global payment messaging standard, its adoption is not always consistent and global standards for payment routing and account identification have not yet been universally adopted. While 85 countries (as of April 2023) make use of the International Bank Account Number (IBAN), many countries, such as the US, the Philippines, Singapore, Brazil, India and South Africa do not for domestic payments. Domestic account numbers in each country have different formats. Proxies may be an answer to this issue, but again, there are many different approaches to what counts as a valid proxy. In some countries, only a mobile phone number is permitted, while others allow a citizen or corporate identifier. The efforts underway by the CPMI to further promote ISO 20022 harmonisation for enhanced cross-border payments are a welcomed initiative.[4]
- **Differences in operational frameworks and scheme rules.** While many countries are willing to have similar operational rules and processes for fast payments, this will not always be the case. There will be areas of potential inconsistency within the detailed scheme rules that may have a negative impact on the end-to-end solution for cross-border payments including mismatches between the domestic scheme versus those needed for international payments, such as in mandatory field usage, permitted values within drop-down lists such as error codes, and rules for handling exceptions. There could also be differences between the domestic schemes on the formats of remittance information, intermediary parties as well as sending and beneficiary accounts. Where inconsistencies arise, agreement needs to be reached in terms of whose rules should take precedence.
- Most FPS are designed with a strong local focus and therefore only support a single domestic currency. The **lack of multicurrency functionality** and, where it is required, cross-currency conversion capabilities introduces costs and frictions when aiming at using the FPS for facilitating cross-border payments. The overwhelming majority of FPS systems around the world support only their local currencies as their focus has historically been on domestic payments. This may pose a challenge for these systems to introduce efficient cross-border payments as foreign exchange (FX) frictions will emerge. Only very few countries and regions have implemented multicurrency FPS as the feasibility of supporting multiple currencies in a domestic system largely depends on the existence of high-volume payment corridors to support the return on such investment.
- **Ambiguity and inconsistency in governance and oversight** leads to uncertainties over the delineation of responsibilities between the scheme owner, technical operator and PSPs, impacting contractual obligations and legal certainty. Such differences can be key barriers to interlinking go-live, scale and viability. This will not only influence the governance and

[4] CPMI (2025): *BIS CPMI takes further steps to promote ISO 20022 harmonisation for enhanced cross-border payments*, January.

contractual obligations of an interlinking arrangement, but also the willingness of payment system participants to serve in these roles and utilise the linked arrangement for cross-border payments.

Different domestic systems are governed by local central banks, private entities or a mix of both. Aligning these governance structures is complex. For instance, in the UK Faster Payments is operated by Pay.UK, while TIPS is governed by the Eurosystem and FedNow is governed by the Federal Reserve. Each FPS has distinct operational rules and oversight mechanisms, leading to potential conflicts or inefficiencies in global interoperability.

Governance approaches involving multiple checks and approvals throughout the processing chain can create friction and delay time-sensitive payments for end-users. Decisions made at the interlinking arrangement level may have knock-on implications for participants and other users, including but not limited to changes in processes and protocols, investments in infrastructure, technology and staff as well as changes in pricing and fees.

The CPMI has outlined considerations to the governance for interlinking of domestic FPS for cross-border use and has set out recommendations for oversight by authorities.[5] The report notes that oversight of FPS interlinking arrangements will have to rely on cooperation among overseers of component FPS – particularly in areas of common interest related to the structure and functioning of the interlinking arrangement.

A lack of a common regulatory and compliance approach represents another barrier to the efficiency of interlinked FPS. A key barrier to interlinking is the lack of a common regulatory approach, specifically in the area of sanctions compliance, misaligned customer due diligence (CDD), data protection and regulatory reporting. AML and countering the financing of terrorism (CFT) regulations vary significantly between countries and common practices are lacking.[6] The know your customer (KYC) regulations and guidelines are challenging to navigate from one country to another and electronic KYC (e-KYC) guidelines are even less aligned. PSPs can interpret the requirements differently, depending in part on their risk appetite. This may lead to variations in screening procedures and the level of risk they are willing to accept. Some of the specific challenges related to AML and sanctions screening include:

- Complex and ever-changing sanctions lists that often contain inconsistent or poor-quality information.
- Risk of false positives – on average, a false match against the sanctions list will result in a 24-hour delay to the payment.
- Lack of resources and/or suitable expertise to effectively implement and manage sanctions compliance programs.
- Difficulties of ongoing monitoring of customer transactions, behaviour and risk profiles.
- Siloed approach that hinders the aggregation of data across systems, divisions and geographic locations.

---

5 CPMI (2024): *Linking fast payment systems across borders: governance and oversight – Final report*, October.

6 While the rules of the Office of Foreign Assets Control (OFAC), the financial intelligence and enforcement agency of the US Treasury Department, which administers and enforces economic and trade sanctions, are commonly applied worldwide, they remain US-originated standards without legal standing unless they have been transposed into domestic law. Similarly, the European Union (EU) standards are applied within the EU and in other countries, but there is no obligation for the standards to be used in non-EU countries. Each country will also have their own standards, which may or may not overlap with OFAC standards. If sanctions are applied without international coordination, this can leave PSPs scrambling to comply with a very wide range of different sanctions.

- Lack of shared frameworks for cross-border fast payments to screen transactions more effectively.
- Data protection rules, which place restrictions on sharing data, often create a conflict with the requirement to screen payers and payees using high-quality verified data that cannot be shared outside the country. In addition, it may be a breach of privacy laws to screen data against (a) specific list(s), where it is not the law of a particular country.

Domestic payment systems typically settle in local currencies. Cross-border payments require real-time FX processing, subject to regulatory scrutiny on transparency and accuracy of rates. In many countries, there are expectations on reporting trade- or currency-related information to regulators for cross-border transactions. This information may include the amount of payment, the parties involved in the payment, the purpose of the payment, and transaction volumes. In particular, the purpose classification of a payment can be challenging because there is often no consistent usage between countries.

While the international payments business unit of a PSP will have expertise in this area, this knowledge and experience is often not shared or available to the domestic payments part of the PSP. The hierarchy of specific laws and regulations applicable to interlinking arrangements can result in ambiguity or even potential conflicts of law and regulation. The jurisdictions involved in an interlinking arrangement also need to find a common understanding of the regulatory obligations of all parties (which is not the same as a common legal standard).

Without identifying and addressing the key contributing frictions, there is a danger that industry will focus their efforts on areas that may bring only marginal improvements and not address the true root causes where significant gains can be achieved. The frictions in the *final* leg of cross-border payments have been set out in a recent report by Swift.[7]

- **Managing multiple stakeholders.** The complex nature of cross-border payments means that multiple parties are likely to be part of the transaction flow. Key stakeholders include central banks, PSPs, technology providers and regulators, each with varying priorities. Coordinating these stakeholders can be a significant barrier for establishing an interlinking arrangement and its day-to-day operations as it can add friction and create challenges in meeting time frames required for an end-to-end real-time processing.

  Depending on the design of the cross-border solution, the payer's and the beneficiary's PSP would need to connect to FX providers, liquidity providers and intermediary service providers, all of whom need to have connections that enable dialogue and decisions within time frames required for an end-to-end real time flow. Many PSPs, especially smaller banks, may lack the technical infrastructure to support cross-border fast payments, creating bottlenecks. Ultimately, these challenges create complexity, add costs and create frictions for FPS operators and PSPs can also result in poor end customer experiences:

  - End users may be subject to hidden fees in currency conversion. End users may unknowingly incur high FX fees during cross-border payments, as conversion rules differ between schemes. Transparency issues can lead to dissatisfaction.
  - End users may experience payment delays due to compliance holds. In certain jurisdictions compliance holds can incur delays. The end user expects instant settlement but experiences frustration due to unclear processing timelines.

[7] Swift (2024): *Spotlight on speed. Where to focus for faster international payments*, October.

- Customer payments maybe rejected due to data mismatch. For example, an end user inputs their address in a UK format (postcodes), which does not align with the data requirements of an FPS abroad, leading to a rejected transaction without clear feedback on the error. This can be hopefully eliminated if there is agreement between schemes to use structured address formats.
- The risk of fraudulent transactions across the entire arrangement increases if one of the FPS has weak fraud controls. Like in other cases, the safety of the weakest component determines the safety of the overall network. The FPS in the interlinking arrangement with the weakest fraud controls can, therefore, compromise the entire network, thereby eroding end user trust.

4. INVENTORY OF SELECTED FPS

The number of FPS in operation continues to grow, with an estimated 88 FPS in place as of Q4 2024 The PIE Task Team 2 has undertaken a stocktake across all geographic regions, resulting in an inventory of 54 FPS (covering about 60% of FPS currently in operation). The inventory is based on publicly available data and offers valuable insights into FPS interlinking opportunities. It can serve as a basis for industry collaboration going forward.

In a rapidly evolving environment, the details included in the inventory are subject to change. For instance, in February 2025, the Federal Reserve announced plans to increase the maximum transaction limit for USD fast payment transactions on FedNow to USD 1 million, effective from summer 2025. Additionally, the inventory data is sourced on a 'best efforts' basis with certain challenges encountered in sourcing comprehensive details for each FPS. As such, the inventory is intended to be a 'live' database, evolving over time to serve as an important tool for advancing FPS interlinking. It can also be viewed in the context of similar initiatives such as the Project FASTT,[8] to provide a broader perspective on the opportunities unlocked by FPS.

4.1 FPS inventory analysis

To understand the global FPS landscape and to gauge potential for FPS to support cross-border payments, the PIE Task Team 2 conducted a stocktake of FPS, identifying their core design features that could support cross-border payment capabilities. The results indicate that of the 54 FPS:

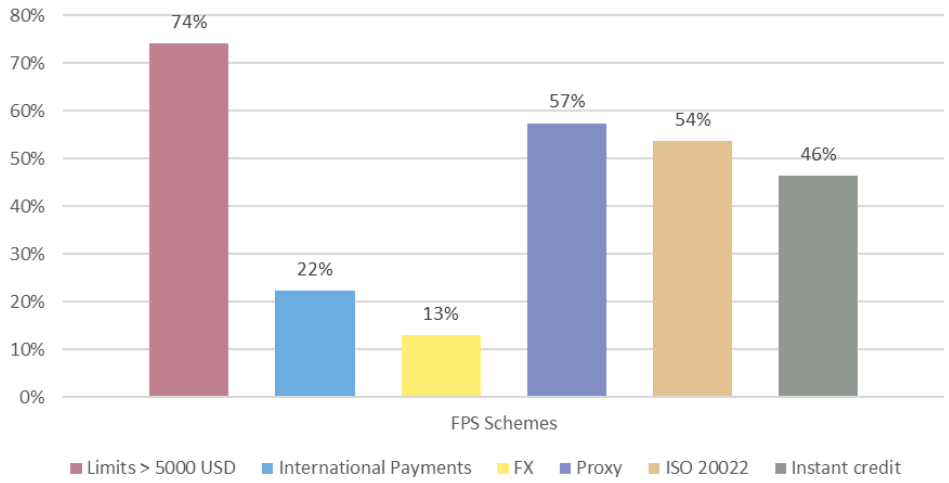
- 20 have the ability to accept cross-border payments (37% of total);
- 16 have the ability to send cross-border payments (30%); and
- 38 use ISO 20022 (70%).

Using these design features as 'reference indicators', alongside a median daily transaction cap limit of at least the equivalent of USD 5,000, Task Team 2 determined the 'readiness' of an FPS for interlinking. Based on this approach, approximately **half of the 54 FPS would have the potential to process cross-border payments.** While challenges remain, as outlined in this report, the findings highlight a significant opportunity to leverage the current FPS landscape for interlinking to advance cross-border payments.

A more detailed analysis of the key features of the 54 FPS is provided below. This analysis focuses on FPS capabilities to send and receive international payments, cross-border payment limits applied across jurisdictions, supported use cases, message formats and institutional access to FPS. FPS that have several key features – daily limits of USD 5,000 or higher, cross-border capability, FX provision, instant availability of funds and ISO 20022 compliance – is taken a 'ready' for cross-border transactions

[8] World Bank: *Project FASTT (Frictionless Affordable Timely Transactions)*.

Figure 1: FPS 'readiness' for cross-border transactions



Source: PIE Task Team 2 analysis as of Q4 2024 on 'best efforts' basis drawing on publicly available information.

Ability to receive and send international payments. While additional data on FPS and their ability to send and receive international payments will be required to better analyse this design feature, it is worth noting that the number of FPS supporting the receipt of international payments is slightly higher than those supporting the sending of outward payments. The reasons may include factors such as capital account controls, AML/CFT requirements, and domestic currency internationalisation policies.

In many cases, receiving international payments through an FPS requires less requirements, as long as a correspondent bank to assist overseas participants in currency conversion and act as an agent to complete the remittance. Correspondingly, in order to support the sending of international payments through an FPS, it is necessary to consider at least including the FX channels, the method for determining the exchange rate, the handling of chargebacks due to settlement failures and other such tasks require a collaborative mechanism. Therefore, compared to FPS that support international receipt, sending is a more challenging task.

Table 2: FPS ability to accept and send international payments

Region	Ability to **receive** international payments			Ability to **send** payments international payments			
	Yes	No	No data	Yes	No	No data	
Africa	0	5	13	0	5	13	
Asia & Middle East	8	5	1	7	6	1	
Europe	8	5	-	7	6	-	
North America	2	1	-	1	1	1	
Oceania	1	-	-	-	1	-	
South America	1	5	-	1	5	-	
total	20	21	14	16	24	15	

Source: PIE Task Team 2 analysis as of Q4 2024 on 'best efforts' basis drawing on publicly available information.

Use cases supported by the FPS. Based on the analysis, FPS primarily support cross-border payment scenarios aimed at person-to-person (P2P) transactions, including international remittances, travel payments, and payments for studies abroad. Specific uses that can be extended to cross-border applications include invoice and utility payments or wage payments to foreign bank accounts. The analysis identified 19 FPS that support cross-border use cases, including merchant payments and international remittances. Additionally, a few FPS support wholesale payments. Examples, in the

domestic context for now, include Fawateer in Bahrain and Pagos al Instante BCRD in the Dominican Republic.

Access to the FPS. Among the 34 FPS (for which information on participating institutions is available), 32 provide direct or indirect access for non-bank PSPs. These include electronic money institutions, payment institutions, wallet providers, and remittance service providers. These firms are required to meet certain conditions, obtain a specific payment license, or operate within the scope of certain regulatory frameworks, such as the new European Instant Payments Regulation. However, further work is required to better understand the requirements and processes for non-bank PSP to gain either direct or indirect access to FPS. This includes analysing whether these requirements are proportionate or pose challenges for the non-bank PSPs to meet. Such requirements are not necessarily solely determined by the FPS. They can be influenced by the legal and regulatory framework of the country in which the FPS operates (such as the National Payment System Act) and the PSP licensing regimes in place for non-bank PSPs.

Message format. Among the 54 FPS analysed, 38 systems (70%) have fully or partially adopted the ISO 20022 message standard. Additionally, eight systems (15%) use the ISO 8583 message standard, while five systems rely on proprietary protocols. It is expected that ISO 20022 will continue to play an important role in cross-border interlinking of FPS.

Table 3: Analysis of message formats used in FPS

Region	Typical information standard				Total
	ISO 20022	ISO 8583	Proprietary	No data	
Africa	8	6	2	2	18
Asia & Middle East	13	-	1	-	14
Europe	12	1	-	-	12
North America	2	-	-	1	3
Oceania	1	-	-	3	1
South America	3	1	2	-	6
total	38	8	5	6	54

Source: PIE Task Team 2 analysis as of Q4 2024 on 'best efforts' basis drawing on publicly available information.

FPS cross-border payment limits. FPS transaction limits, both for domestic and for cross-border payments (where applicable), vary significantly across jurisdictions. These limits are shaped by a combination of credit risk considerations, market demand, and regulatory requirements. Most FPS impose restrictions on payment amounts within an operational day, while others implement different types of caps. Some limit single payment amounts (such as CliQ in Jordan),[9] some have annual total amount limits and others rely on self-imposed limits agreed upon by directly participating institutions (such as the FPS in the UK).[10] In certain cases, options exist to exceed these limits. This may involve drawing additional credit from commercial banks or from the respective central bank (including advanced customer qualifications) or higher-level credit certification within the FPS.

A detailed analysis of daily transaction limits, usually imposed by FPS scheme rules, reveals significant variation. For instance, jurisdictions in Asia typically have limits equivalent USD 1,500 a (see section 4.2), while other jurisdictions have limits equivalent to USD 5,000. This variation calls for a further analysis of current transaction limits and their implications across various use cases and payment corridors in the context of G20 Roadmap.

9 JoPACC: *CliQ Features*.
10 Pay.UK: *Transaction limits*.

4.2 FPS transaction limits: analysis of selected jurisdictions in Asia

The rationale behind FPS transaction limits varies depending on the operator and the context in which the limits are applied. In some cases, limits are set by the central bank as FPS operator, with a focus on the support of the FPS (such as PromptPay in Thailand). In other cases, limits are determined by commercial banks or payment institutions, which consider factors such as their own risk appetite and customer profiles (such as PayNow in Singapore).

An analysis of transaction limits in several Asian jurisdictions, including Thailand, Singapore, Malaysia, Hong Kong SAR and India, where FPS cross-border interlinking is relatively mature and cross-border use cases are similar (merchant payments via QR codes and remittances), indicates the daily limit of cross-border payment per person is generally about USD 1,500 (see Table 4).[11]

Using publicly available data, the analysis highlights the key distinction between transaction limits in domestic and cross-border payments. The 'default transaction limits' allowed by local FPS or FPS participating institutions, without requiring additional credit or adjusting the limit, serve as reference standards.[12] Additionally, the analysis finds that specific use cases, such as QR code-based payments to merchants or personal remittances, often have their own transaction limits applied.

Table 4: FPS transaction limits in selected Asian jurisdictions

FPS	Jurisdiction/ regions and currency		Payment transaction value limits	Average exchange rate in 2023	Typical daily default limit*
PromptPay	Thailand	THB	Limit depends on the cross-border country connected with. The default limit is 50,000 THB (=1,436 USD) per day, beyond which face authentication is required (Since April 2023, BOT).	USD/THB= 34.80	1436.78
FPS	Hong Kong	HKD	Subject to participants (Banks & Stored-Value Facility operators (SVF)) The default limit is 10,000 HKD (=1,277 USD) or 10,000 CNY per day.	USD/HKD= 7.83	1277.14
PayNow	Singapore	SGD	SGD 2,000 (=1,492 USD) per day. *Mobile banking is 1,000 Singapore dollars per day.* *Online banking 1,000 Singapore dollars per day.*	USD/SGD= 1.34	1492.53
DuitNow	Malaysia	MYR	MYR 3,000 (=658 USD) for cross-border payments per transaction. The individual limit in DuitNow Maybank / ICBC Malaysia is 5,000 MYR (=1,096 USD) per day (equivalent to domestic facilitation quotas).	USD/MYR= 4.56	1096.49
UPI	India	INR	The UPI transaction limit per day for an account holder has been defined in UPI network from bank to bank. Mainstream banks adopt a daily limit of INR 100,000 (=1,210 USD) per day per account. INR 1,00,000 per day per account is the limit for domestic transaction. Specific limits are defined for cross-border linkages. For example, currently the limit for India-Singapore linkage is SGD 1,000 per transaction/per day.	USD/INR= 82.60	1210.65

* USD equivalent, indexed to 2023 average exchange rates

Source: PIE Task Team 2 analysis as of Q4 2024 on 'best efforts' basis drawing on publicly available information.

[11] Differences in reported FPS payment limits reflect varying perspectives: CIPS focuses on default cross-border operability limits for individual users, while Buna emphasises system-level functional limits. Data are drawn from central banks, commercial banks or non-bank PSPs. Data should be interpreted within the context of actual credit conditions for meaningful analysis.

[12] Bank of Thailand: *Cross-Border Payment Linkages*; HSBC: *Pay abroad with FPS | Cross-border Payments*; DBS: *PayNow FAQs*; UOB: *Transfer money overseas*; OCBC: *PayNow Help & Support*; Cashfree: *UPI Transaction Limit in India 2025: Everything You Need to Know*

5. CROSS-BORDER FAST PAYMENTS – SELECTED CASE STUDIES

There are multiple approaches to leveraging FPS for cross-border payments, of which FPS interlinking is one. This section presents several of these approaches through specific initiatives:

- **PromptPay**: Serves as an example for bilateral FPS interlinking.
- **Buna**: A central platform solution that enables interlinking between participating countries' FPS.
- **PAPSS (Pan-African Payment and Settlement System)**: A multilateral payment scheme that facilitates cross-border payments within and across African nations using local currencies.
- **European Payments Council's (EPC's) OCT Inst scheme**: A "one leg out" scheme that enables cross-border fast payments.
- **UPI (Unified Payments Interface)**: Enables interlinking and is already connected with several FPS globally.
- **Nexus**: Offers a multilateral approach to FPS interlinking.

5.1 PromptPay FPS interlinking

PromptPay, Thailand's FPS, has significantly advanced financial inclusion by enabling real-time, low-cost transactions through proxy account identifiers, such as national ID numbers and mobile phone numbers. Driven by strong government support, the initiative has achieved widespread adoption, further enhanced by the integration of QR code payments. This innovation has significantly accelerated the transition to digital transactions, both within Thailand and through QR code-based payment interoperability with eight other jurisdictions. PromptPay's cross-border link with Singapore's PayNow, marked in 2021 the first bilateral FPS bilateral interlinking arrangement. This milestone enabled instant, low cost cross-border transfers, enhancing regional financial integration and delivering interoperability.

5.2 Buna central platform solution

Buna is a multilateral and multicurrency payment system. While being cross-border by design, Buna is pursuing to interlink with other FPS. Buna enables eligible financial institutions, central banks and payment systems to send and receive cross-border payments in real-time. It supports US Dollar (USD), Euro (EUR), Emirati Dirham (AED), Saudi Riyal (SAR), Egyptian Pound (EGP) and Jordanian Dinar (JOD). Buna's network currently includes more than 100 participants from various jurisdictions. It has developed multiple interlinking models to connect with domestic FPS and RTGS systems around worldwide, leveraging its "leg-in/leg-out" scheme for efficient integration. Buna has an embedded financial crime compliance (FCC) programme and operates under a cooperative oversight framework of multiple central banks. Buna is operating PvP mechanism for FX settlement, adopting a harmonised approach for ISO 20022 messaging.

5.3 PAPSS – the Pan-African Payment and Settlement System

PAPSS is a multilateral cross-border payment system designed to facilitate real-time payments across Africa using local currencies. By enabling transactions in local currencies, PAPSS minimises unnecessary dependency on foreign currencies while sending/receiving cross-border payments between African countries. The platform enables both direct and indirect participation, provided participants adhere to PAPSS scheme rules, including its bylaws, credit rule book and membership agreement. PAPSS supports a number of local currencies of its African Members and settles the net in hard currency via the local

central bank or a commercial bank.[13] As of January 2025, PAPSS had 155 direct participants, including central banks, commercial banks, national switches and other connectivity providers, from 15 African countries. PAPSS is also pursuing interlinking opportunities with other payment systems across the globe to enable fast payments between the African continent and the rest of the world.

5.4 EPC OCT Inst – the "one leg out" instant credit transfer scheme

The EPC launched the "One-Leg Out Instant Credit Transfer" (OCT Inst) scheme, which is specifically designed for international instant credit transfers. Unlike an interlinking arrangement, OCT Inst is a payment scheme, ie a multilateral agreement that binds both the EPC and the schemes participants. The scheme is governed by a rulebook that sets out functional rules, practices and standards to achieve interoperability for the provision and operation of the euro leg of an international instant credit transfer, as agreed at the inter-PSP level within the Single Euro Payments Area (SEPA). OCT Inst provides a set of business and functional payment exchange rules ("rulebook") and a set of technical specifications ("implementation guidelines"). These are based on ISO 20022 (2019 version) and only apply to the euro leg of the instant credit transfer. Each scheme participant retains the freedom to determine how it manages its clearing, settlement, FX and liquidity processes for both incoming and outgoing OCT Inst transactions. The scheme is open to all PSPs located in 41 jurisdictions that are part of SEPA. The EPC additionally also offers to license its OCT Inst scheme to other interested communities in line with its intellectual property policy and based on fair, reasonable, and non-discriminatory terms.

5.5 UPI instant payment system and protocol

UPI is a system that integrates multiple bank accounts into a single mobile application (from any participating bank), offering a unified platform for various banking features, seamless fund routing and merchant payments. Developed by the National Payments Corporation of India (NPCI) in 2016, UPI has revolutionised India's digital economy by enabling seamless, real-time payments via mobile devices. Its user-friendly design – facilitating transactions through virtual payment addresses and QR codes – has driven widespread domestic adoption across both urban and rural areas. Government support and zero-cost transactions have propelled UPI to process billions of monthly transactions, encompassing P2P, person-to-merchant (P2M) and utility payments. Internationally, UPI's bilateral partnerships have expanded its reach to countries such as Bhutan, Singapore, Nepal, Sri Lanka, the United Arab Emirates, Mauritius and France. These collaborations enable cross-border P2P and P2M transactions

5.6 Nexus multilateral approach

Nexus is a multilateral FPS interlinking initiative designed to enhance the speed, cost-efficiency, transparency and accessibility of cross-border payments by connecting domestic FPS globally via a single hub developed by the BIS Innovation Hub. It improves the approach of bilateral linkages, as Nexus offers a scalable and sustainable approach by enabling each FPS to establish a single connection to the Nexus platform, which then facilitates seamless access to all other FPS in the network. Using standardised protocols such as APIs and ISO 20022, along with a comprehensive scheme rulebook that streamlines rules across jurisdictions, Nexus minimises the complexity of managing diverse requirements. This approach enhances the efficiency of transaction processes while ensuring interoperability. Nexus also introduces a financially sustainable model, offering strong incentives and flexibility for participants to join, fostering a unified and inclusive global payment network. The BIS Innovation Hub has worked with the central banks and payment system operators in India, Malaysia, the Philippines, Singapore and Thailand to validate and evaluate the Nexus model. Nexus Global

[13] PAPSS: A 7-minute guide to PAPSS.

Payments (NGP) was established in May 2025 by the central banks and FPS operators of India, Malaysia, the Philippines, Singapore, and Thailand. NGP is a not-for-profit organisation incorporated in Singapore, which is dedicated to managing the Nexus scheme and advancing fast, efficient, and safe cross-border payments at scale. With NGP at the helm, Nexus has transitioned from a BIS-led initiative to an independent and collaborative effort.

6. FPS INTERLINKING FOR CROSS-BORDER PAYMENTS – CONSIDERATIONS AND SUGGESTED NEXT STEPS

Interlinking of FPS for cross-border use will require practical approaches that can work across diverse jurisdictions and payment schemes. This will involve leveraging common practices, striving for regulatory harmonisation, and coordinating effectively across points of divergence. Such interlinking efforts should take advantage of the network effects created by mutualised investments, ensuring benefits for all participants in the payment chain, while maintaining scalability to handle increasing transaction volumes efficiently and economically. Continued innovation and competition will play a key role in delivering better solutions, reducing transaction fees, improving customer service and lowering costs for end users. However, this process should be supported by commercial viability to ensure that participants have a clear business case and a commercially sustainable market. Proportionate and appropriate public sector support will also be important.

To fully unlock the potential of FPS interlinking, it is crucial to ensure that both existing and new arrangements enable fast and secure transactions, while maintaining reliability and adaptability to the evolving needs of the financial sector. The industry considerations and suggested next steps directed at FPS owners and operators, PSPs and public authorities, are ambitious in scope. Taking them forward will require collaboration and coordination among stakeholders. In particular, detailed work will be necessary to develop a pragmatic, sequenced, and proportionate approach. This must account for account for competing priorities, be carefully assessed for unintended consequences, and be grounded in thorough analysis and consultation.

6.1 Enable all domestic fast payment schemes and systems rules to send and receive cross-border payments

To enable interlinking and multicurrency arrangements, FPS operators should review their domestic schemes to address functionality and processes needed for cross-border payments. This could require technical changes, revisions to scheme rules, changes to governance procedures and participation contracts, and an assessment of the commercial viability.

The implications of enabling cross-border payments in a domestic scheme are complex and wide ranging. It is therefore necessary for the FPS operators to assess the optimal approach in the context of their systems, operational priorities and customer requirements. As operators upgrade and renew their domestic fast payment processes and systems, priority should be given to enabling cross-border payments. This could include interlinking arrangements, one-leg-out arrangements, and multicurrency features. Ideally, existing FPS participants should be able to send and receive cross-border transactions without requiring a new onboarding process (as demonstrated by the example of Iberpay).[14] While sending cross-border payments should be optional for PSPs, FPS and their participating PSPs should be able to receive cross-border payments.

[14] Iberpay views cross-border payments as simply another use case for instant payments. Recognising that cross-border payments require further information and that a separate rulebook exists for these transactions in SEPA, Iberpay has

6.2 Foster FPS interoperability through continued alignment to common standards

The interoperability of technical elements among participants in an interlinking arrangement, as well as the ease of achieving such interoperability, will impact the time to market, adoption, scalability, and overall viability of such arrangements. FPS participants may need to make significant investments (both in terms of time and resources) to align existing messaging standards, processes, technologies, and infrastructure to join an interlinking arrangement. Interoperability considerations include, but are not limited to, differences in messaging standards and settlement timeframes (as domestic schemes may define "instant" differently), and use of specific technologies (such as cloud solutions for data storage).

The primary focus is on enabling instant credit transfers. However, as interlinking arrangements evolve, a broader range of use cases could be supported. These services may include confirmation of payee, account resolution, aliases, request to pay, and QR code payments. Since these services may be provided as part of the FPS or by the same operator, they can be incorporated into standardisation efforts when FPS are interlinked.

Back-office operations and processes that should porgress towards interoperability include approaches for recalls, returns, investigations, dispute resolution, fraud management practices, sanction screening, and allocation of liabilities. Services such as liquidity optimisation or data analytics may be more challenging to standardise as they are specific to the FPS operator. However, as the demand for interoperable services grows, it is expected that commercial service providers will begin to introduce solutions to the market to address these needs.

Further collaboration between the industry and public sector is required to promote consistency and transparency in end-to-end transaction data to support use cases. For example, refunds require sender information, which is not consistently available in transaction data across all jurisdictions.

The increasing adoption of ISO 20022 will facilitate interoperability. The need for its consistent use is explored further in a CPMI report on ISO 20022 harmonisation, which highlights the importance of common standards and usage guidelines in achieving interoperability.[15] Without such standards, each interlinking arrangement may develop bespoke solutions, resulting in a variety of integrations that increases complexity and cost.

Momentum towards increased messaging standardisation comes from the developments around HVPS+[16] and the reactivation of the Instant Payments Plus (IP+)[17] working group, which aims at creating guidelines for leveraging fast payments at a cross-currency level. These efforts, along with other bridging tools like request-to-pay and worldwide adoption of ISO 20022, underscore the importance of aligning domestic FPS upgrades with international standards. Harmonising ISO 20022 implementation and market practices will be essential as these systems are reviewed or enhanced.

6.3 Provide reciprocity (similar service propositions on both sides of a cross-border transaction) at a reasonable cost

Reciprocity in an FPS interlinking arrangement means that end users on both sides of a cross-border transaction benefit from similar service propositions, whether sending or receiving payments across jurisdictions. This concept is central to achieving interoperability from the customer's perspective, though the level of reciprocity required may vary depending on individual channels or domestic service levels (see Annex A for further details on reciprocity). The implementation of reciprocity goes beyond

---

developed a superstructure. This superstructure integrates both instant credit transfers and cross-border credit transfers, aiming to process cross-border payments in a manner similar to purely domestic instant credit transfers.

15 CPMI (2023): *Harmonised ISO 20022 data requirements for enhancing cross-border payments – final report*, October.

16 Swift: *High Value Payments Systems Plus*.

17 Swift (2024): *Harmonising instant payments for a global payments ecosystem,*

technical interoperability between FPS and includes the necessary legal and business arrangements that ideally ensure similar end-user service propositions. This includes consistent user experiences for payments sent and received across jurisdictions.

As cross-border fast payment services are usually optional rather than mandatory for participants in local FPS, operators should define and agree on the level of reciprocity with their participants and regulatory authorities in the relevant jurisdictions. Reciprocity for FPS interlinking arrangement may include processes for dispute resolution, fraud handling, FX conversion, and settlement arrangements. However, services required for cross-border payments, such as FX conversion, compliance requirements and additional payment information may require significant adjustments to domestic systems. A phased approach is recommended to implement reciprocity arrangements, taking into account market demand and desired customer outcomes, while ensuring that reciprocity is provided at a reasonable cost to maintain the commercial viability of interlinking services. Finally, it is also noted that some payment corridors may experience a significant proportion of one-way transactions (eg certain regions/countries with predominantly incoming payments), where reciprocity may be less relevant.

6.4 Prioritise harmonisation of anti-money laundering (AML) checks and sanctions screening while preserving their highest effectiveness

Addressing the need to harmonise AML and sanctions screening requires considerable effort, as the requirements, procedures, methods, and actions vary across jurisdictions. However, these differences pose significant challenges for participants in payment systems. Harmonisation of AML requirements and sanction screening procedures by the public sector would increase alignment across jurisdictions. This would prevent PSPs from having to conduct multiple, varied screenings for the same transaction to meet jurisdiction-specific requirements. Such harmonisation, particularly across interlinking arrangements, would enable the private sector to screen more efficiently, reducing unnecessary frictions and costs in processing cross-border payments. In this context, PIE Task Team 2 believes that the FATF can play a pivotal role in driving high-level harmonisation across AML and sanctions screening practices.

Furthermore, sanctions screening methods and the actions to be taken should be consistent across jurisdictions. For example, the requirement to screen client databases in addition to transaction-based screening adds complexity and increases costs and processing times. Moreover, the actions to be taken, such as blocking funds versus returning a transaction, should be harmonised. A significant improvement could be achieved if intermediary banks were not required to screen transactions twice when both the originating and beneficiary banks are using a domestic or regional instant payment system and are already conducting the necessary screenings. To further enhance efficiency, in specific use cases where the beneficiary has undergone pre-screening – such as a merchant, similar to practices in the card payment industry – screening requirements for PSPs should be limited. This would allow cross-border fast payments to follow procedures similar to those of card transactions.

Different frameworks must align requirements related to documentation and proof of identity used for KYC, permissions for customer data usage through eKYC, ongoing monitoring for CDD, and institutional due diligence standards among PSPs. Adjusting approaches, legislation, and regulation related to AML and sanctions screening will require time. It is recommended that further work be undertaken to explore detailed alternatives. With the support of new technologies that improve and enable automation of processes while ensuring robust data privacy and security, and with global supervision and oversight models in place for various entities, including Swift and CLS, PIE Task Team 2 believes there is an opportunity to create a safe harbour agreement in the AML and sanctions space. Such an agreement could be applied globally while remaining adaptable. Harmonisating international best practices and promoting the widespread use of automation are clear paths to improving AML and sanctions screening.

Regulatory harmonisation could generate significant gains for the entire cross-border payment value chain. Harmonisation, through the alignment of relevant laws and the reduction of regulatory grey areas, would benefit all participants in the payments ecosystem by promoting competition, reducing costs, and increasing transaction speed.

6.5 Increase access for non-bank PSPs to FPS based on the principle of "same activity, same risk, same regulation"

An increasing and varied number of non-bank PSPs offer cross-border payment solutions based on FPS interlinking. While these firms drive innovation and competition, they are not always eligible to become direct FPS participants, may lack access to central bank money, and can face challenges in establishing indirect FPS access through relationships with other PSPs.

Non-bank PSPs frequently serve underbanked or unbanked populations by providing alternative payment solutions. Expanding the options for non-bank PSPs to participate in FPS, whether through direct or indirect access, will help to diversify use cases, address gaps in customer access, and further financial inclusion goals. This expansion will also foster a more competitive payments ecosystem, encouraging innovation, reducing transaction costs, and enhancing the quality of payment services. The decision by non-bank PSPs to access FPS will depend on their risk appetite, market strategies, and business models, enabling them to leverage their agility and rapid innovation to benefit the ecosystem and deliver value to end users.

PIE Task Team 2 believes that both, FPS operators and current FPS participants, should be open to sending and receiving cross-border payments from non-bank PSPs, provided all compliance requirements are met. Anecdotal evidence indicates that, in certain cases, receiving PSPs have rejected payments based on the type of sending PSP rather than the results of a compliance check, adding complexity and reducing transparency for the end user. PIE Task Team 2 believes that, at a minimum, non-bank PSPs should be granted access to payment systems through indirect arrangements. FPS operators should provide a clear pathway for non-bank PSPs to gain direct access. Onboarding procedures, technical requirements, and integration standards should be designed to make the process efficient and straightforward. Direct FPS access would provide non-bank PSPs and their customers with greater certainty that payments will be sent and received, thereby supporting the G20 target for transparency.

Central banks and other authorities should have a more open licensing regime that facilitates direct access for non-bank PSPs to FPS, in the view of PIE Task Team 2, reducing their dependency on direct participants to settle transactions in central bank money. Currently, non-bank PSPs often rely on local banks for clearing and settlement of cross-border payments due to economic considerations. Aligning with the Wolfsberg Group's emphasis on payment transparency, the FPS scheme management should define the payments in scope and implement standards that ensure full transparency of all parties involved in the payment chain. PIE Task Team 2 considers that direct access to central bank money would expand market choice, lower overhead costs associated with indirect participation and further enable non-bank PSPs to drive innovation and competition. In some jurisdictions, access to FPS is only permitted to entities that are regulated financial institutions holding accounts on the central bank's books.

Increased access comes with increased obligations and oversight. Non-bank PSPs with access to FPS and central bank accounts must operate under the principle of "same activity, same risk, same regulation." This would ensure that the same micro prudential regulation, oversight regimes, and supervision apply to both PSPs and non-bank PSPs with direct FPS access. Payment systems operate with security and resilience as fundamental priorities. FPS that are interlinked for cross-border payments should ensure that no undue risks are introduced by the interlinking arrangement. Balancing the need to manage risks with the goal of broadening reach and access will require a proportionate, risk-based

approach to payments systems access. Several reports outline the opportunities, challenges, and the role of the public sector in supporting non-bank PSPs' access to payments systems.[18]

6.6 Adjust fast payment transaction value limits to support expanded use cases and higher-value payments

While transaction value limits for fast payments help manage fraud and liquidity risks, they can also create a barrier to evolving market demands, broader participation and market development, particularly for new use cases like higher-value B2B transactions.

To fully realise the benefits of interlinked FPS, industry stakeholders and authorities must address several key considerations. First, fast payment transaction limits should be adjusted or eliminated to accommodate diverse payment types, such as B2B, C2B, P2P transactions. At the same time, advanced fraud prevention tools, such as pre-validation, must be implemented to ensure the secure handling of higher-value transactions. Additionally, 24/7 liquidity availability needs to be ensured through coordination with liquidity providers to support continuous operations. Settlement models, including net, pre-funded, or deferred settlement, should be evaluated to determine their suitability for higher-value payments. Finally, legal frameworks might require updating to enable the processing of high-value transactions by FPS.

By raising transaction limits and expanding use cases, FPS can unlock new opportunities for cross-border and high-value payments. This could drive market adoption and broader participation while meeting evolving demands. Sending PSPs should have the flexibility to determine their transaction limits based on their own risk appetite and business models. Similarity, receiving PSPs should be able to accept fast payments of any value, provided they comply with the regulations of the local jurisdiction. At a minimum, fast payment schemes should have sufficiently high transaction value limits to enable a wide range of use cases through interlinking.

6.7 Address the e-commerce use case

FPS interlinking should address the clearing and settlement of a broad range of use cases. Among these, the adoption of a clearly defined and cohesive approach to the cross-border e-commerce use case by FPS operators will help drive transaction volumes, increase the economic benefits of implementing interlinking arrangements and reduce system costs. However, not all FPS are adequately prepared to support the e-commerce use case, which requires several essential ancillary processes. These include dispute resolution, chargebacks, facilities for refunds, and mechanisms for handling liability and data, such as those needed to support the reconciliation of return payments. Without these processes in place, e-commerce service may lack the robustness required to build consumer confidence in this payment method and provide the necessary functionality for merchants. Dispute resolution services and procedures to manage chargebacks will be particularly critical.[19]

The adoption of international good practice models for buyer and merchant protection guarantee schemes, chargebacks and dispute management/refunds – similar to those used by card processors – will enhance both customer and merchant confidence in the use of fast payments in e-commerce. For PIE Task Team 2 further analysis is needed to explore the implications of developing

---

[18] For example, CPMI (2022): *Improving access to payment systems for cross-border payments: best practices for self-assessments,* May.

[19] A chargeback occurs when a customer requests the reversal of a transaction, resulting in the return of funds used in a purchase, for example due to a commercial dispute.

similarly cohesive, best-practice propositions for e-commerce use cases within FPS interlinking arrangements.

6.8 Support proxies and aliases, such as mobile phone numbers, and wallets to increase customer access

Proxies and aliases are recommended to validate sender and receiver account details, irrespective of whether a country uses IBAN or not. They can reduce friction by improving data quality, lowering costs by avoiding transaction repairs, enhancing the customer experience, and playing a key role in increasing consumer access to payment services. Harmonisation of aliases should be encouraged to foster the use of mobile phone numbers or alternative aliases (such as email addresses, IDs, or disposable aliases) for cross-border payments, where the validation of sender and recipient parties is critical.

In certain markets, mobile phone numbers may offer an increased level of KYC, making them a viable alias at a global level. However, it is unnecessary to mandate a specific type of alias. Instead, aliases of various forms should be supported to provide flexibility. For instance, an individual may prefer not to share their phone number. While some jurisdictions allow for the use of IDs (in India, for example, UPI IDs act as proxies for transactions routed through the UPI FPS), in others IDs might not be widely available.

If mobile phone numbers are utilised as aliases for enhanced KYC purposes, there could be an opportunity for telecommunication companies to play a role in confirming the details of mobile phone numbers used as aliases. This could assist with KYC processes and provide intelligence on fraudulent or scam numbers. To mitigate risks associated with mobile phone numbers, such as scams, phishing, and unauthorised access, some FPS have implemented virtual addresses or aliases. These provide an additional layer of security and privacy, offering a potential alternative for countries globally. This approach enables secure financial transactions while safeguarding sensitive personal information.

In other markets, wallets are mainstream access channels and are essential for facilitating financial inclusion. In these markets, interoperability between the proxies and aliases used by FPS and wallet providers, as well as other value-added payment services, is important. Addressing privacy and security concerns is crucial for building user trust. Establishing globally standardised practices and promoting secure alternatives will enhance user confidence and facilitate widespread adoption of mobile phone number as proxies, fostering financial inclusion and improving the cross-border payment experience.

Existing domestic proxy/alias resolution services will need to be adapted to support cross-border use cases, including cross-border confirmation of payee. This will require secure, standardised data sharing across borders with trusted counterparts based on reciprocity (see section 6.3). Public sector support will likely be necessary to address the challenges of cross-border data sharing for payment pre-validation purposes. Additionally, solutions such as privacy-enhancing technologies could be explored to mitigate privacy concerns.

6.9 Facilitate a cross-border information exchange to combat fraud

In the context of FPS interlinking, managing unhappy paths, particularly in relation to fraud and scams, and the subsequent recovery of funds, is a critical component of ensuring safety and trust in the arrangement. Actors across the ecosystem have an active role to play in this effort. Industry participants should actively share current domestic practices for detecting fraud and establishing recovery paths between institutions to build a collaborative and efficient framework. By mapping these practices against various use cases and jurisdictions, stakeholders can identify gaps and inconsistencies in fraud management and recovery processes. This collective effort can then be used to develop a comprehensive set of recommendations tailored to different players across the ecosystem, enhancing fraud prevention, detection, and recovery across borders. Such collaboration will ensure that when fraud

or scams occur, there are well-defined recovery paths in place, minimising financial loss and maintaining confidence in the payment system.

In addition to the complex network of financial institutions and service providers involved in cross-border payments, PIE Task Team 2 considers that the broader ecosystem involved in FPS interlinking should share the liability and responsibility for preventing fraud. Firms such as telecommunication companies, social media platforms, and other entities that play a role in the digital transaction environment, can mitigate potential risks associated with fraud, scams, and operational disruptions, which can impact both individuals and institutions. Furthermore, as many providers already operate cross-border, they have additional tools and data that can support the detection and elimination of cross-border fraud.

Central banks and regulators have a crucial role in fostering a safe and stable financial environment, ensuring that the entire ecosystem operates securely and efficiently. Regulators can help build a framework that ensures trust and stability in the financial system. This collaborative approach not only mitigates risks but also enhances confidence in the system, enabling both industry stakeholders and individuals to rely on real-time, cross-border payments with assurance. Authorities, in particular, have a role to play in defining the roles and responsibilities of all stakeholders in the cross-border payment chain to maximise security and trust. An accompanying report by Task Team 2 on addressing fraud in cross-border payments sets out the Task Team's considerations for the private sector and calls for support from authorities in combatting fraud in the context of cross-border payments. The World Bank has also issued a report fraud prevention techniques, which could be taken into account by the PIE task force in its future work.[20]

Public and private sector dialogue and concerted effort are required to facilitate cross-border information exchange to mitigate fraud. This includes addressing issues such as common fraud data taxonomies, a data model for confirming the payee, information sharing, and the legal/policy limits on such sharing. Additionally, the wider ecosystem should play a role in minimising fraud at its source.

6.10 Prioritise increasing alignment of governance and oversight frameworks between FPS interlinking arrangements

Governance, commercial, and technical models should incentivise adoption and promote the scale and viability of the interlinking arrangement. However, many barriers to FPS interlinking are related to the need for alignment between jurisdictions on the underlying governance, commercial, and technical models of linked arrangements. Potential disputes arising from payment errors, information requirements, timeouts, or fraud highlight the need for a consistent approach to governance. Differing legal jurisdictions complicate these issues – for instance, a payment error originating in one jurisdiction but affecting a beneficiary in another may fall under conflicting consumer protection laws. Governance frameworks should be based on principles of neutrality and inclusiveness to promote the long-term viability of linked arrangements. To address these challenges, interlinked FPS arrangements should incorporate harmonised and transparent dispute resolution mechanisms that are adaptable across jurisdictions. These mechanisms should include clearly defined roles and escalation paths for handling disputes, whether arising from technical failures, fraud, or consumer issues, to ensure timely and fair resolutions.

Effective risk management frameworks are also essential to address potential legal, financial, and operational risks associated with interlinking FPS. This includes establishing clear legal foundations, robust financial risk mitigation strategies, and comprehensive operational risk controls to ensure the safety and efficiency of cross-border payments. Achieving the desired end state may require balancing the roles and responsibilities (and thereby control) between regulators, scheme owners, technical

[20] World Bank (2023): *Fraud risks in fast payments*, October.

operators, and FPS participants. For example, what is mandated by regulation in one jurisdiction may equate to a commercial contractual arrangement in another. As domestic schemes are extended to embrace interlinking and achieve desired outcomes, payment system participants should be consulted from the very beginning of the development process.

Increasing alignment of governance and oversight frameworks, based on a clear division of responsibilities between public authorities, scheme owners, technical operators, and FPS participants is essential to support the increasing scale, required harmonisation, and ambitions for FPS interlinking. The CPMI has published detailed considerations FPS interlinking governance and oversight, which can serve as a foundation for public and private sector dialogue to advance several Task Team 2 considerations laid out in this report. [21]

7. CONCLUSIONS

Interlinked domestic and regional FPS for cross-border payments represent a significant and tangible opportunity, as evidenced by the inventory compiled and analysis undertaken by the PIE Task Team 2. Realising the full potential of FPS to meet the G20 Roadmap for cross-border payments will require considerable and coordinated effort between public authorities and the private sector to address the challenges that could inhibit this potential. These challenges extend beyond the technical requirements for interconnection, as many factors influencing interlinking are partly outside the sphere of influence of the FPS owners.

A continued move toward coordinated activities is essential, alongside the adoption of standards. These standards should encompass technical and payment messaging, supported usage guidance, cohesive operational frameworks, and rules. Additionally, consistent governance and oversight are necessary, along with the harmonisation of rules across jurisdictions related to screening. Addressing these foundational supports for FPS will enable the private sector to continue innovating FPS interlinking for cross-border payments that are fast, accessible, at reasonable cost, and ultimately support desired customer outcomes.

FPS operators should enable their systems to both send and receive cross-border payments. By addressing challenges related to the e-commerce use case and enabling broader use of aliases and proxies, FPS operators can improve customer access. To expand access to a broader customer base, often serviced by non-bank PSPs, FPS operators should expand options for non-bank PSP to have direct or indirect access to the FPS. Similarly, the public sector should support greater access to FPS for non-bank PSPs on the basis of "same activity, same risk, same regulation" (and ideally the same regulator). Maintaining trust and integrity in FPS is critical, and the public sector should facilitate the cross-border exchange of information to combat fraud. Furthermore, the broader ecosystem (such as telecommunication companies and social media platforms) should recognise their role and responsibility in preventing fraud.

To increase speed, FPS owners and operators, in consultation with PSPs, must foster system interoperability by continually aligning with common standards. Transparency should also be a priority. PSPs and FPS owners should encourage reciprocity at a reasonable cost, delivering a consistent user experience for end users on both sides of a cross-border payment transaction. This includes ensuring similar service propositions for cross-border payments. FPS operators should enable the adoption of proxies and aliases, where supported in local systems, for cross-border payments as well. This will reduce friction and improve the customer experience.

---

[21] CPMI (2024): *Linking fast payment systems across borders: governance and oversight – final report*, October.

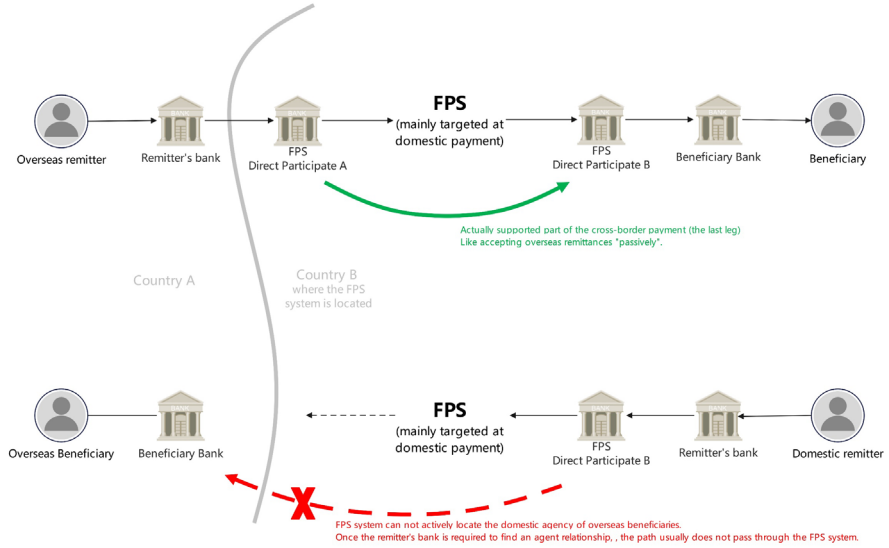
Reducing costs is another critical area of focus. The public sector should prioritise harmonising AML and sanctions screening processes, to increase efficiency and reduce the operating costs for PSPs. Additionally, efforts should focus on aligning governance and oversight frameworks. Both the public and private sectors should undertake detailed work to explore adjustments to approaches, legislation, and regulations related to AML and sanctions. This includes assessing technologies that support automation, applicability and harmonisation of international best practices. Greater harmonisation and alignment in AML and sanctions screening will also help increase speed as most delays are due to screening requirements.

Annex A: Reciprocity

Reciprocity, as a concept, refers to mutual recognition between two or more parties for their shared benefit. In the context of processing cross-border payments through interlinking FPS, reciprocity ensures that end users on both sides of a transaction benefit from similar service propositions for payments sent to and received from a counterparty in another jurisdiction. The specific level of similarity required for reciprocity must be agreed upon and may vary depending on the individual channels or domestic service levels.

This annex provides a brief overview of reciprocity in the context of cross-border payments, highlighting how it could contribute to the current G20 cross-border payments roadmap. It aims to address some of the challenges posed by the lack of reciprocity in such arrangements. Reciprocity in cross-border payment arrangements applies when the sending and receiving institutions are separate entities located in different jurisdictions. This is particularly relevant for two types of FPS interlinking arrangements, ie multilateral interlinking of domestic FPS and bilateral linkages between FPS (eg through a scheme arrangement).

Figure A.1: Stylised overview of reciprocity concept



Source: PIE Task Team 2

Cross-border FPS interlinking arrangements rely on service level propositions of the domestic solutions in place and "topology" of the respective communities.[22] These service levels and topologies differ. Furthermore, the parties involved on either side of a solution offering a degree of reciprocity can differ. For instance, in a bilateral interlinking arrangement, reciprocity would exist be between the FPS operators (domestic or regional) that agree to provide one another with mutually acceptable processing conditions. In a multilateral arrangement, an FPS operator (or a participant) would establish an agreement with a central party that ensures reciprocity with other FPS that also maintain a relationship with the same central party.

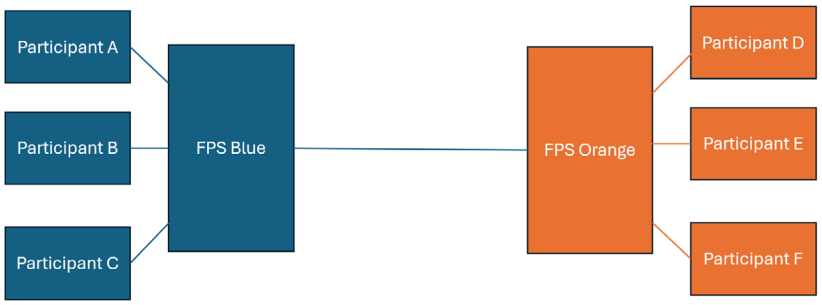
Reciprocity should provide mutually agreed levels of similarity of treatment for all users across the payments chain. It goes beyond technical interoperability between systems to include the necessary

[22] The topology of a "hub and spoke" network such as UK FPS, US RTP is different to a multi-layer/provider network like SCTinst in the EU and again like the distributed network in Australia. Points of entry to these networks may be significantly different and need to be resolved in any multi-lateral cross-border model.

legal and business arrangements that enable cross-border payments to be made with transparency, speed, and at a reasonable cost by a wide range of users. A basic premise of the "guarantee of reciprocity" is the ability to send, and the expectation to receive payments by or through the PSP.

In Figure A.2, participant A has the right to send to and receive payments from participants B and C as a result of them all being participants in FPS Blue. Under a bilateral interlinking arrangement that includes a reciprocity arrangement between FPS Blue and FPS Orange, Participant A would also be able to send payments to and receive payments from participants D, E and F.

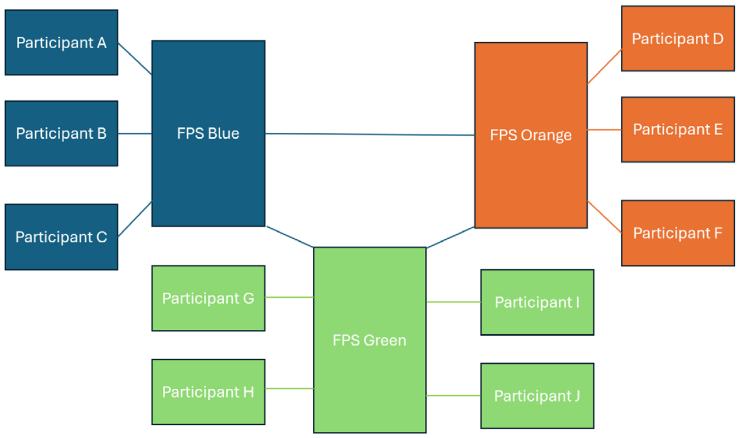
Figure A.2: Representation of a bilateral FPS interlinking agreement that includes a reciprocity arrangement



Source: PIE Task Team 2

In Figure A.3, participant A has the right to send to and receive payments from participants B and C as a result of them all being participants in FPS Blue. Under a multilateral linkage arrangement that includes reciprocity between FPS Blue, FPS Orange and FPS Green, participant A would also be able to send payments to and receive payments from participants D, E, F, G, H, I and J.

Figure A.3: Representation of a multilateral FPS interlinking agreement that includes a reciprocity arrangement



Source: PIE Task Team 2

Full reciprocity is neither a right nor a given, and the level of reciprocity may need to be agreed between all or some of the FPS, their participants and the regulatory authorities in the different jurisdictions. Appropriate legal arrangements would be required to underpin the reciprocity agreement, inclusive of assurances as to the legal status and regulatory compliance of the PSPs involved in the transaction. Reciprocity is premised on the basis that PSPs will be ready to send and receive payments ("readiness") under the agreed processing conditions, using pre-agreed standards, and will be able to process pre-agreed use cases.

Table A.1: Processing arrangements required to enable reciprocity

Messaging standards and usage guidelines	Fraud management practices, sanction screening and allocation of liabilities	Data requirements
Happy and unhappy paths, including recalls and returns	Security standards, BCP/DR, incident management	Governance of change management
Investigations and disputes process	FX conversion and settlement arrangements	Availability and accessibility on a 24/7 basis

Source: PIE Task Team 2

A reciprocity arrangement should not be expected to establish commercial arrangements for participants, though charging practices may be included, as is the case in SEPA, where the scheme mandates full principal amount being received by the beneficiary. As a result, no BENE D (deduction from beneficiary amount) is allowed in SEPA schemes. Any cross-border reciprocity arrangement will cover transactions that go across different regulatory regimes and, as such, regulatory alignment by policymakers is an important enabler. This includes addressing currency controls that can hinder the ability to make cross-border payments.

Further, there are some caveats to the basic premise. For example, there may be some corridors where the majority of payments actually go in one direction (for example, a remittance corridor where migrants send money back to their home country) – thus tempering the need for two-way reciprocity (although the need to be able to return payments may need a level of reciprocity to be in place). Reciprocity could also be affected by the relative importance of certain use cases or payment types. For example, low dollar value remittances may dominate in some corridors while others enable higher value payments to support trade.

Annex B: Case studies of FPS and schemes supporting cross-border payments

PromptPay

PromptPay is overseen and regulated by the Bank of Thailand (BOT) under a robust regulatory framework and ongoing supervision. The Payment Systems Committee (PSC) formulates access and governance rules to ensure alignment with national and international standards. Risk management measures address significant risks, supported by continuous oversight. Stakeholder collaboration, interoperable infrastructure, and public awareness initiatives by BOT promote trust and confidence in digital payments. Service levels and scheme rules are developed by the payment industry, including PSPs and infrastructure operators, under BOT guidance and in line with international standards. PromptPay is operated by NITMX, ensuring security, reliability, speed, and robustness. Data security is prioritised through encryption and private network communication. Participants must comply with BOT regulations and hold a payment services license.

For cross-border payments, settlement banks manage FX and settlement risks, conducting currency conversions. Operational resilience is ensured through compliance with BOT's IT risk policies, with business continuity and disaster recovery plans in place. PromptPay has adopted the ISO 20022 messaging standard, enabling real-time AML/CFT screening. Its approach to cross-border connectivity focuses on establishing a strong user base before expanding collaborations. Challenges such as jurisdictional differences are addressed through harmonisation or finding compromise solutions. Fraud risk is managed via NITMX's Central Fraud Registry, while liability is outlined in service agreements. BOT ensures consumer protection through market conduct guidelines and a contact centre for reporting issues.

Table A.2: PromptPay features

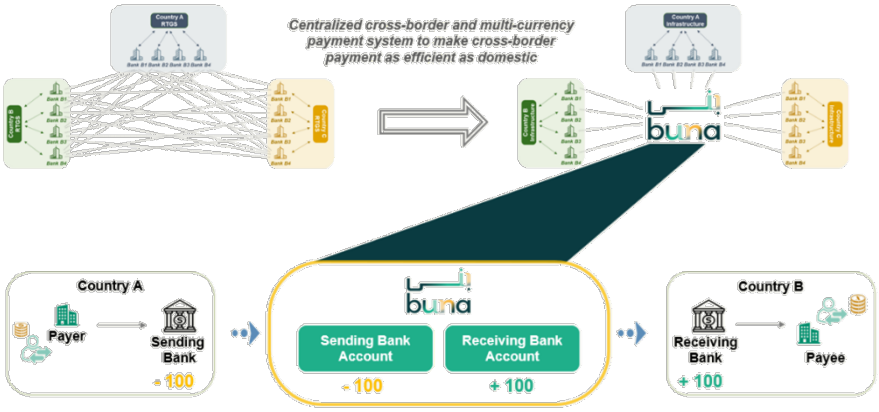
Function	Related features
Liquidity management	Intraday credit facilities are not applicable to PromptPay. PromptPay transactions are settled via the RTGS system, BAHTNET. While transactions are processed in real time for customers, PSPs settle on a deferred basis, utilising netting of credit and debit positions to save liquidity. BAHTNET also offers a dedicated portal for participants to manage their collateral within the system.
Payment messaging	PromptPay uses standardised messaging based on ISO 20022. For personal data protection, it employs a two-step proxy-lookup system, maintaining a registry of telephone numbers linked to service providers, with the operator redirecting instructions to the appropriate provider for account holder information. NITMX provides an API infrastructure to support product and service development, with participants required to comply with NITMX's API standards. PromptPay operates 24/7/365, ensuring continuous availability.
Compliance and data processing	Thailand's Anti-Money Laundering Office (AMLO) mandates real-time sanction screening for cross-border payments. NITMX adheres to a data governance policy that complies with personal data protection laws.
Clearing	PromptPay operates on a single-cycle model with one net settlement per day.
Settlement	Legal finality is ensured under the Payment System Act, safeguarding completed payments within the system. PromptPay operates on a deferred net settlement basis, with settlements conducted in Thai Baht using central bank money as the settlement asset. Credit risk is mitigated by requiring participants to pledge additional collateral equivalent to their historical debit positions.
Foreign exchange (FX)	Currency conversion is managed by a single settlement bank, which maintains FX liquidity and mitigates FX risks through a nostro account, providing all FX quotations for transactions within the corridor. Payment versus payment (PvP) is not applicable.

Source: PIE Task Team 2

Buna

Buna, launched in 2020, is a multilateral cross-border and multi-currency payment system initiated by Arab central banks. It promotes economic integration, financial inclusion, and stronger ties with global partners, operating under the Principles for financial market infrastructures (PFMIs). Buna addresses inefficiencies in cross-border payments, offering real-time transactions for over 100 banks across 15 countries in six major currencies, with additional currencies being added.

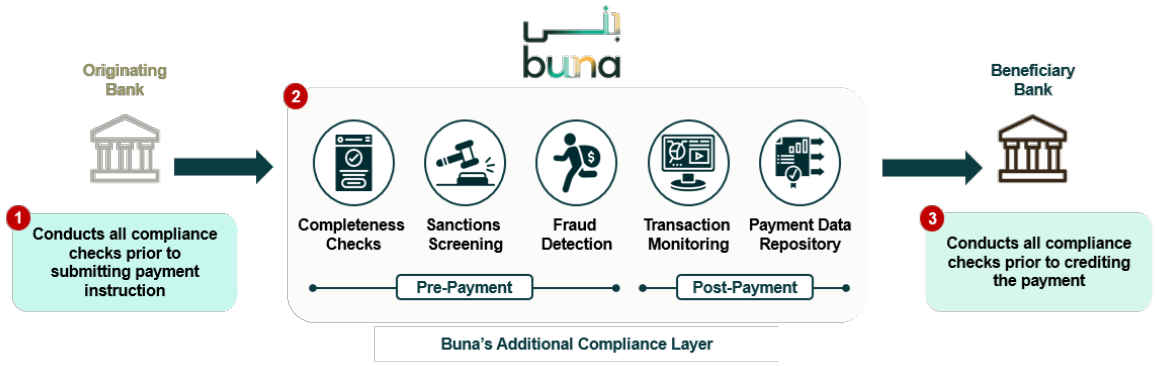
Figure A.4: Buna model



Source: Buna

Buna ensures compliance with international AML/CFT standards through strict participation criteria and due diligence processes. Transactions undergo data checks, sanctions screening, fraud detection, and monitoring.

Figure A.5: Buna's compliance approach



Source: Buna

Buna's interlinking model supports instant remittances and enables participants to connect financial institutions across networks, facilitating multi-currency payments with end-to-end visibility. The interlinking model is based on the Buna leg-in/leg-out scheme, which is designed to allow processing one leg of the payment through Buna while the other leg is either initiated or received in another eligible network. The scheme enables participants to link other financial institutions (including own branches and subsidiaries) to channel their multi-currency payments in an efficient way with full end to end visibility.

- Model 1 – network to network interlinking: a network will onboard to Buna as a participant, the local currency will be included in Buna, and transactions will be processed in the same currency.
- Model 2 – central bank collaboration: the central bank will onboard to Buna as a participant and funds holding institution, the local currency will be included in Buna, and transactions will be processed in the same currency.
- Model 3 – commercial bank(s) collaboration: collaboration between banks that participate in Buna and another payment systems to achieve interlinking, transactions can be processed in the same currency or in multiple currencies with the interlinking bank(s) providing the FX conversion.

Key features include multiple currencies, embedded compliance, ISO 20022 support, and Swift connectivity. Liquidity management is centralised, with participants funding accounts in advance or intra-day. Buna also facilitates PvP transactions, optimising liquidity and creating new business opportunities.

Table A.3: Buna features

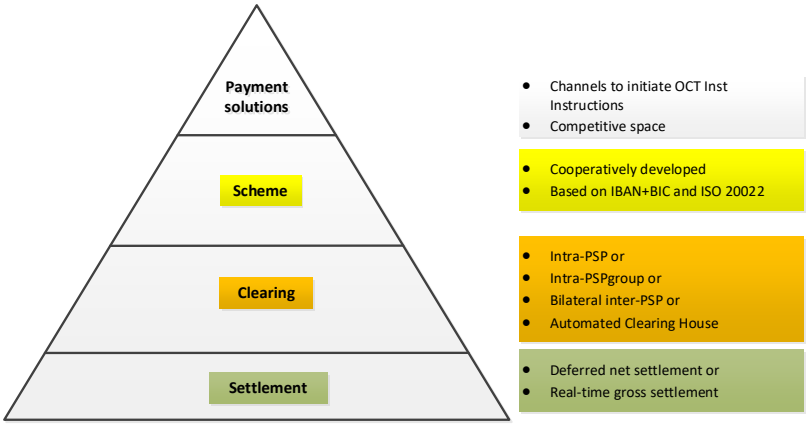
Functions	Related features
Liquidity management	Participants can project their liquidity needs in advance and fund their accounts either ahead of time or intra-day. Buna's centralised model eliminates liquidity risk by ensuring that transactions cannot be processed without sufficient funding. Depending on the currency, participants can fund their accounts in Buna through their local in-country RTGS system, correspondent banks, or the Buna PvP option. The Buna PvP option functions as a marketplace, enabling participants to use their available liquidity (balances in different currencies) to perform FX transactions directly with one another. This approach has helped participants optimise liquidity costs and unlock new business opportunities within the ecosystem.
Payment messaging including authentication, initiation, submission and conditionality	Buna supports ISO 20022 and utilises the Swift network for connectivity, ensuring compliance with the Swift Customer Security Programme (CSP). It is ISO 27001-2022 certified, reflecting its strong commitment to information security. Additionally, Buna offers overlay services such as CAS management and pre-validation APIs, which operate over secure VPN connections to enhance functionality and security.
Compliance and data processing	Buna operates across multiple jurisdictions with an independent supranational setup and a multilateral model governed by a unified framework of rules and procedures. Its cooperative oversight framework includes multiple central banks, whose currencies are part of the system. Buna has implemented an effective financial crime compliance (FCC) programme, which is built on three key pillars: (i) governance, roles and responsibilities; (ii) participant onboarding due diligence; and (iii) robust controls and processes. To enhance safety and efficiency, Buna has voluntarily added a second layer of compliance to payment flows, conducting its own checks in addition to those performed by the originating and beneficiary financial institutions. All transactions undergo data completeness checks, sanctions screening, fraud detection, and monitoring. For core payment operations, Buna securely collects and stores data required for settlement, compliance, fraud checks, billing, and other obligations, leveraging Swift connectivity. For value-added services, such as pre-validation, data retrieval, and FX inquiries, Buna uses a pass-through approach via an API gateway over a secure VPN, ensuring data is not stored within the Buna system.
Clearing	n/a
Settlement	Buna operates using a real-time book-entry settlement model, ensuring that payments settled within the system are final and irrevocable. Liquidity is held in Buna's accounts with fund holding institutions (FHIs), which may be either central banks or commercial banks, depending on the currency.
Foreign exchange (FX)	Buna supports multiple currencies, including USD, EUR, SAR, AED, EGP, and JOD. Transactions are processed in the same currency, such as USD-USD or AED-AED. Currency conversion is handled by participants, either between the participant and their customer for payments or between the participant and their correspondent bank for liquidity purposes. Buna also offers a PvP mechanism to optimise liquidity. This allows a liquidity provider to supply liquidity to a requester based on an agreed FX deal, which is then settled through Buna's PvP service.

Source: PIE Task Team 2

European Payment Council's (EPC's) One-Leg Out Instant Credit Transfer (OCT Inst) scheme

The EPC's OCT Inst scheme is a multilateral agreement binding participants to a set of business and functional rules outlined in a rulebook. The scheme supports 24/7/365 processing and adopts ISO 20022. Participants are responsible for developing their own channels and services for OCT Inst transactions.

Figure A.6: Different payment processing layers



Source: EPC

The scheme's rulebook defines service levels, including a recommended 60-second processing time for the euro leg. Currency conversion and financial risks are managed transparently, with risk measures outlined in a risk management annex (RMA). Operational resilience is ensured through the RMA, which includes measures to address business and information security risks.

Table A.4: EPC OCT Inst features

Function	Related features applicable to the euro leg – the non-euro leg is outside the scope of the OCT Inst scheme
Liquidity management	Outside of the scope of the OCT Inst scheme.
Payment messaging including authentication, initiation, submission and conditionality	The OCT Inst scheme uses the 2019 version of ISO 20022. Proxy-lookup registries and pre-validation services are optional. Multiple commercial solutions are available, ut are outside the control of the EPC. APIs for technical integration are not specified, as the scheme relies solely on ISO 20022 XML messages. The scheme supports 24/7/365 transactions, ensuring continuous availability. Processing execution timelines are defined at the scheme level, and a maximum transaction amount of 100,000 EUR per instruction is applied under the scheme's capital flow management measures.
Compliance and data processing	The OCT Inst scheme rulebook establishes clear eligibility criteria for entities wishing to adhere to the scheme. These entities must comply with AML, CFT, KYC, and data protection laws applicable within the European Economic Area or equivalent national legislation in non-EEA SEPA jurisdictions. The RMA outlines specific measures and recommendations to ensure compliance and mitigate associated risks.
Clearing including netting (where applicable)	There is a clear separation between this layer and the rulebook layer. Each OCT Inst scheme participant has the discretion to organise this layer according to its own preferences and requirements.
Settlement	There is a clear separation between this layer and the rulebook layer. Each OCT Inst scheme participant has the flexibility to organise this layer as it sees fit.

Foreign exchange (FX)	The OCT Inst scheme is agnostic regarding whether, how, where in the payment chain, and by whom the currency conversion is performed, provided that all details of the currency conversion are disclosed transparently.

Source: PIE Task Team 2

Unified Payments Interface (UPI)

India's UPI integrates multiple banking features into a single mobile application, enabling seamless fund routing and merchant payments. Governed by the NPCI, UPI incorporates risk management into its framework, evolving with market conditions and regulations. Scheme rules and service levels are developed through stakeholder consultations and formalised in the Steering Committee. UPI ensures secure, real-time payments through compliance screening, consent management, and pre-validation processes. Settlements are conducted in destination currency to mitigate cross-currency risks. Operational resilience is maintained through defined recovery objectives, while proprietary messaging standards align with ISO 20022 for international compatibility, as seen in the UPI-PayNow linkage between India and Singapore. Fraud risk is managed through AI and ML-based detection systems, with public awareness campaigns enhancing user education. Customer protection is governed by Reserve Bank of India (RBI) guidelines, encompassing grievance redressal, dispute resolution, and fraud liability.

Table A.5: UPI features

Functions	Related features
Liquidity management	NPCI ensures liquidity and manages credit exposures through its settlement guarantee mechanism (SGM), supported by a settlement guarantee fund (SGF), which enables seamless settlement of obligations. Liquidity-saving mechanisms are implemented through settlements conducted via RTGS accounts held by participant banks at the RBI. Only highly creditworthy banks are accepted for prefunding arrangements. NPCI also maintains a separate SGF with alliance partners and conducts daily monitoring of prefunding accounts to ensure adequate liquidity. For collateral management, NPCI collects cash collateral from participants to support the SGF, further enhancing the resilience of the settlement process.
Payment messaging including authentication, initiation, submission and conditionality	UPI uses proprietary messaging formats that are compatible with international standards, such as ISO 20022. Proxy-lookup registries and pre-validation services are available to enhance functionality and security. APIs are provided for seamless technical integration with third parties, supporting real-time operations. UPI operates 24/7/365, with time limits for processing defined in its technical specifications.
Compliance and data processing	Each regulated entity is required to comply with the capital flow management guidelines issued by the RBI. NPCI requires participating members to adhere to RBI regulations, AML/KYC guidelines, and procedural standards. Its fraud risk management system provides real-time fraud detection and prevention across all online products, serving as a value-added service for member banks. While KYC registries are not applicable, NPCI prioritises the security of IT infrastructure, information, and digital identities by employing advanced technologies to ensure data privacy and security. Its robust cybersecurity framework complies with global standards, including PCI DSS v4.0, ISO 27001, ISO 22301, and ISO 27701. NPCI also adheres to PCI DSS requirements, conducts regular audits, and follows global best practices for managing personally identifiable information.
Settlement	NPCI employs a multi-cycle, multilateral settlement model. Under the Payment and Settlement Systems Act, 2007, NPCI ensures legal and technical settlement finality in accordance with its SGM policy and procedural guidelines. Cross-border settlements are governed by agreements between NIPL and network partners. NPCI uses deferred multilateral net settlement, which becomes final and irrevocable once netting is complete, with relevant policies communicated during participant onboarding. Settlements are conducted in Indian Rupees (INR) using commercial bank money as the settlement asset. Settlement risk is mitigated through prefunding, the SGM, and a loss sharing mechanism. The SGF, funded by member banks based on transaction throughput, addresses liquidity

	shortfalls and ensures timely settlements. In cases of default, additional contributions from surviving members and a committed line of credit (LoC) ensure uninterrupted settlement processes. Defaults are reported to the RBI and member banks.
Foreign exchange (FX)	Currency conversion is managed by the remitting side.

Source: PIE Task Team 2

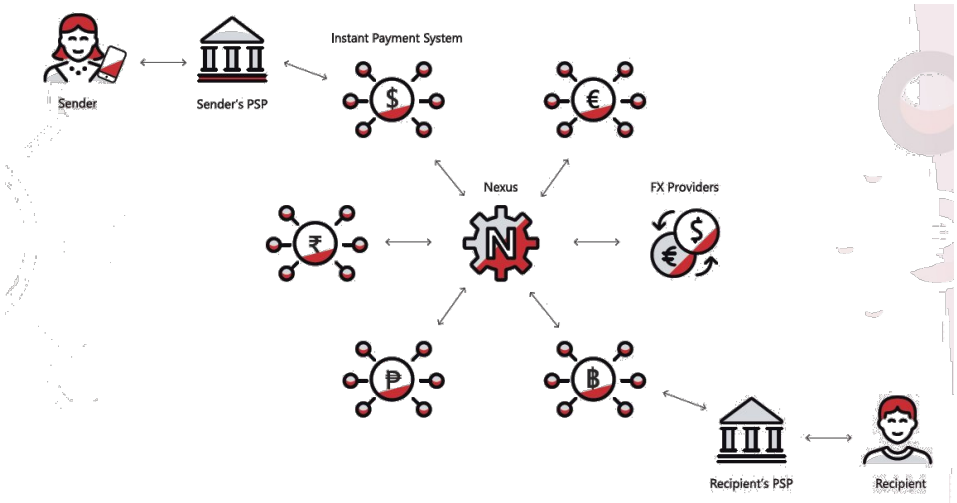
Nexus

Nexus, developed by the BIS Innovation Hub in collaboration with central banks and FPS operators, aims to transform cross-border payments by connecting domestic FPS globally. Starting with central banks from India, Malaysia, the Philippines, Singapore, and Thailand, the Nexus Global Payments (NGP) entity in Singapore manages the scheme. Nexus enhances speed, cost-efficiency, and accessibility in cross-border payments by standardising APIs and ISO 20022 messaging, enabling seamless connectivity across FPS with a single integration. The scheme is scalable, allowing new countries and use cases, such as merchant payments, without additional burdens on existing participants.

The NGP oversees the scheme, establishing rules, eligibility criteria, and dispute resolution mechanisms. A Joint Oversight Forum ensures regulatory harmonisation and information sharing. Nexus supports 24/7/365 operations with robust disaster recovery measures to ensure operational resilience. Its transparent design provides clear guidelines on fees and FX rates, enabling users to make informed decisions before authorising payments. Nexus also adheres to regulatory requirements, including AML/CFT, sanctions screening, and capital flow management measures, ensuring compliance with domestic regulations.

Nexus addresses challenges such as FX risks through flexible currency conversion models that allow PSPs to choose or act as their own FX providers. By enabling payments in under 60 seconds, Nexus offers significant improvements over traditional cross-border payment methods. Furthermore, a standardised dispute portal ensures transparency and fairness in resolving issues between participants. By fostering collaboration between central banks and payment systems, Nexus provides a scalable, efficient, and financially sustainable platform. It simplifies and enhances cross-border payments globally, ensuring accessibility and trust while driving innovation and connectivity.

Figure A.5: Nexus model



Source: BIS Innovation Hub

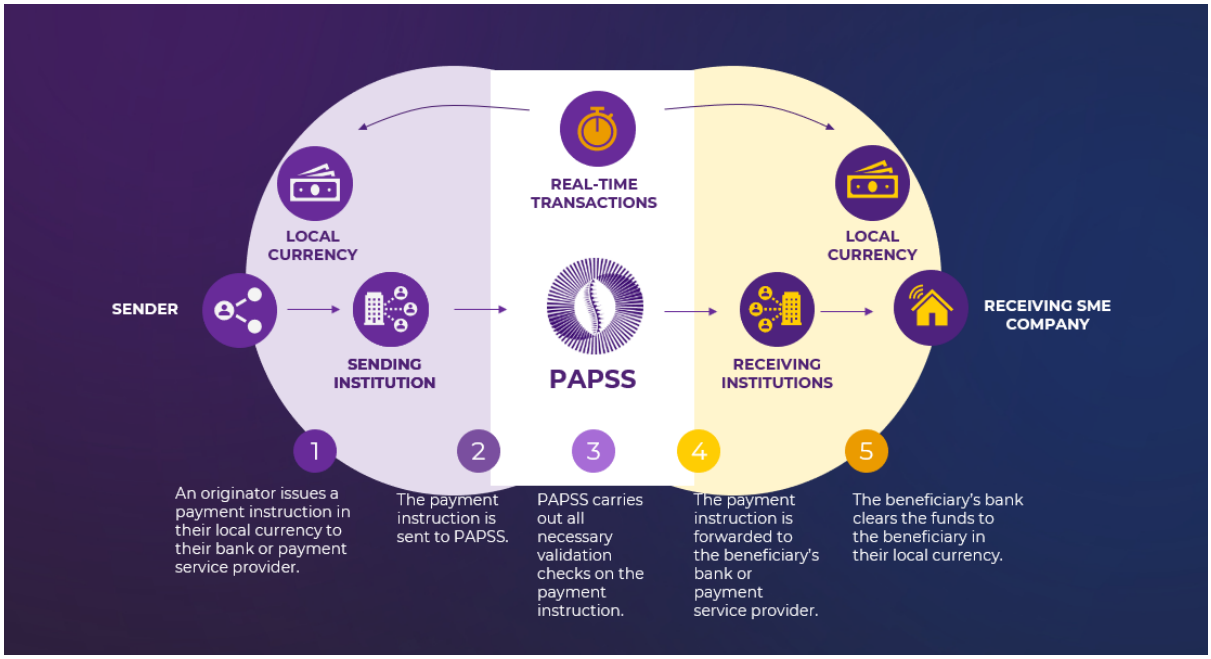
PAPSS

PAPSS, launched in 2021, is a multilateral financial market infrastructure designed to promote Africa's economic and financial integration by facilitating cross-border transactions in local currencies. Its objective is to drive intra-African trade and commerce by making cross-border payments as seamless and efficient as domestic payments. PAPSS supports all African local currencies and settles net positions in USD or other preferred hard currencies. As of January 2025, the platform connects over 155 direct participants, including central banks, commercial banks, national switches, and other connectivity providers across 15 African countries. It also aims to interlink with global payment systems to enable instant payments between Africa and the rest of the world. PAPSS operates on ISO 20022 and adheres to global best practices in AML/CFT, information security, and business continuity, aligning fully with the PFMI.

PAPSS is governed by the PAPSS Governing Council, comprising member central bank governors, and the PAPSS Oversight Committee, made up of directors of payment from member central banks. It ensures compliance with global standards, including FATF Recommendations and Wolfsberg Principles, and maintains a robust AML/CFT framework tailored to the regulatory requirements of African markets. The platform's enterprise risk management framework addresses internal business risks, market dynamics, and stakeholder feedback to ensure its strategies and system enhancements remain aligned with evolving market conditions. PAPSS is certified under ISO 27001, ISO 27701, and ISO 22301 for operational resilience in information security, data privacy, and business continuity.

PAPSS enables instant transactions in local currencies, processed within 7–120 seconds, at competitive costs. It employs a prefunded model to ensure liquidity and supports multilateral net settlement. The platform's ISO 20022 compliance ensures seamless messaging and integration with other systems. By simplifying cross-border payments, PAPSS fosters financial inclusion and strengthens Africa's intra-regional trade and commerce.

Figure A.6: PAPSS operational model



Source: PAPSS

Table A.6: PAPSS features

Functions	Related features
Liquidity management	PAPSS operates on a prefunded model to support its instant payment capabilities. Participants can prefund and defund their accounts based on daily transaction projections and are limited to transacting within their prefunded amounts. Prefunding and defunding are facilitated through Afreximbank or member central bank RTGS systems, depending on whether participants use commercial bank or central bank money for settlement.
Payment messaging including authentication, initiation, submission and conditionality	PAPSS supports ISO 20022, with participants connected to its network via secure VPNs. APIs are exchanged using strong authentication mechanisms and encrypted channels, while 2FA authentication is implemented for transaction monitoring and management interfaces. Transactions are initiated through participants' channels, such as branches, mobile banking, or internet banking, and processed through PAPSS's straight through processing (STP) system. Before processing, several security checks are performed, including prefunded position verification, sanction screening, fraud checks, and validation of the sending bank's certificate for transaction non-repudiation. The beneficiary bank responds with either a positive or negative message, triggering debit and credit actions on the clearing accounts of both banks, ensuring transaction finality. Post-transaction monitoring is conducted to analyse AML behaviour using set rules and AI-driven behavioural analysis. PAPSS is certified under ISO 27001, ISO 27701, and ISO 22301, ensuring compliance with global standards for information security, data privacy, and business continuity. It is also compliant with Swift's Customer Security Program (CSP) and undergoes regular external penetration testing and a bug bounty program to maintain resilience against emerging cyber threats.
Compliance and data processing	The compliance process begins during the onboarding stage, where PAPSS conducts thorough KYC and CDD checks on all participants before they join the network. Post-onboarding, PAPSS performs real-time screening of all transactions against major international sanctions lists, including those from OFAC, the UN, the EU, and the UK. If a potential match is identified, an alert is generated for review, and flagged transactions are initially rejected pending resolution to align with the instant nature of the system. In collaboration with the PAPSS Oversight Committee, regular and risk-based compliance reviews are conducted for participants. These reviews ensure ongoing adherence to industry best practices in AML/CFT, information security, data protection, business continuity, and other critical areas.
Clearing	Clearing on the PAPSS platform is fully automated and conducted in real time.
Settlement	Settlement on the PAPSS platform varies depending on the adopted model: • In the central bank settlement model, participants settle using central bank money. PAPSS opens a settlement account in local currency within each central bank's RTGS. Commercial banks prefund PAPSS in local currency via the local RTGS, and gross settlement occurs in local currencies. Participating central banks prefund Afreximbank in hard currency to enable multilateral net settlement between the countries involved in the transaction. • In the commercial bank settlement model, commercial banks directly prefund their settlement positions in hard currency at Afreximbank, which serves as the settlement bank for PAPSS. Commercial banks set their exchange rates, and net settlement takes place on a multilateral basis among the involved commercial banks. In both models, prefunded positions are reflected in PAPSS as clearing accounts to facilitate transactions in local currency (LCY).
Foreign exchange (FX)	The FX rate is determined by the entity providing the settlement funds. In the central bank settlement model, the FX rate is set by the central bank. In the commercial bank settlement model, the FX rate is provided by the commercial bank, adhering to regulatory guidelines that may vary across markets.

Annex C: Authors and contributors

The main authors of this report are highlighted **in bold,** contributors *in italics*.

Organisation	Name
Iberpay	**José Luis Langa (Task Team co-lead)**
UK Finance, JP Morgan	**Katja Lehr (Task Team co-lead)**
AfricaNenda	*Sabine Mensah*
BUNA	*Deemah Alwazani*
BUNA	*Faisal Alhijawi*
CIPS	*Yang XU*
CIPS	*Shuijiong WU*
CIPS	*Yizheng YING*
Mastercard	**Joy Wann**
Mastercard	*Susan Hall*
NPCI	*Vinod John*
NPCI	*Rina Penkar*
NPCI	*Amit Bajpai*
Pay.UK	*Daniel Jonas*
Societe Generale Group	**Frantz Teissèdre**
Swift	*Mike Truter*
Swift	*Shriyanka Hore*
UK Finance	**Sairoze Hemani**

Annex D: Terminology

Acronym	Definition for the purpose of this report
ADI	**Authorised Deposit-taking Institutions (ADIs)** are financial institutions in some jurisdictions, such as Australia, that are authorised by a financial regulatory authority to accept deposits from the public. These institutions operate under strict regulatory frameworks to ensure the stability of the financial system and the safety of customer deposits Source: Australian Prudential Regulation Authority
AML	**Anti-Money Laundering (AML)** refers to the policies, laws, regulations, and procedures designed to prevent criminals from disguising illegally obtained funds as legitimate income.
API	**Application Programming Interface (API),** is a set of rules or protocols that enables software applications to communicate with each other
CDD	**Customer Due Diligence (CDD)** measures to be taken to identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information; Identifying the beneficial owner; obtaining information on the purpose and intended nature of the business relationship and conducting ongoing due diligence on the business relationship and scrutiny of transactions.
CFT	**Countering the Financing of Terrorism (CFT)** refers to the measures, policies, and legal frameworks aimed at: • Preventing the financing of terrorism. • Detecting and disrupting financial flows that support terrorist groups or activities. Source: Financial Action Task Force (FATF)
EPC OCT	**EPC One-Leg Out Instant Credit Transfer (OCT Inst)** is a cross-currency payment scheme to support the processing of incoming and outgoing international instant account-to-account based credit transfers. It is distinct from other EPC payment schemes as it is the first EPC scheme which covers exclusively the euro leg of international instant credit transfer entering or leaving the geographical scope of SEPA. Source: EPC
FMI	**Financial Market Infrastructure (FMI)** is defined as a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions. FMIs typically establish a set of common rules and procedures for all participants, a technical infrastructure, and a specialised risk-management framework appropriate to the risks they incur. Source: CPMI.
FPS	**Fast Payment System (FPS)** is a payment system that enable the real-time or near real-time transmission of payment messages and the availability of final funds to the payee on as close to a 24/7 basis as possible. Source : CPMI.
IBAN	The **International Bank Account Number (IBAN)** is a code used internationally by financial institutions to uniquely identify the account of a customer at a financial institution as described in the 2007 edition of the ISO 13616 standard "Banking and related financial services - International Bank Account Number (IBAN)" and replaced by the more recent edition of the standard. Source: ISO 20022
IP+	The **Instant Payments Plus (IP+)** Working Group, facilitated by Swift Standards, is a self-standing market practice group of Instant Payment scheme owners/administrators

	that collaborate in the creation/maintenance of the guidelines to provide a building block for harmonising real-time payment systems at both a jurisdictional and cross-currency level.
ISO 20022	**ISO 20022** is a multi-part international standard prepared by ISO Technical Committee TC68 Financial Services. It describes a common platform for the development of messages Source: ISO 20022
KYC	**Know Your Customer (KYC)** is a process used by financial institutions and other regulated entities to verify the identity of their customers, assess potential risks, and ensure compliance with legal and regulatory requirements. It is a critical component of Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) frameworks. **eKYC** is the use of electronic and digital methods to verify identity.
P2P	**Person-to-Person (P2P) payment** is a transaction where both the payer and the payee are individuals.
P2B	**Person-to-Business (P2B) payment** is a transaction where the payer is an individual and the payee is a business.
P2M	**Person-to-Merchant (P2M) payment** is a transaction where the payer is an individual and the payee is a merchant.
B2B	**Business-to-Business (B2B) payment** is a transaction where both the payer and the payee are businesses.
PSP	**Payment Service Provider (PSP)** as an entity that offers payment services, including remittances. This category encompasses banks and other deposit-taking institutions, as well as specialized entities such as money transfer operators and e-money issuers
PvP	**Payment versus payment (PvP)** is a settlement mechanism that ensures that the final transfer of a payment in one currency occurs if and only if the final transfer of a payment in another currency or currencies takes place. PvP transfers can occur within a jurisdiction or across borders. Source: BIS Quarterly Review, March 2020
RTGS	**Real-time Gross Settlement (RTGS)** is the settlement of payments, transfer instructions or other obligations individually on a transaction-by-transaction basis.
SAP	**Settlement Access Provider (SAP)** is a specific role under project Nexus in which a PSP connected to a domestic Instant Payment System provides accounts to FXP that are not members. Source: BIS
SEPA	**Single Euro Payments Area (SEPA)** was introduced for credit transfers in 2008, followed by direct debits in 2009, and fully implemented by 2014 in the euro area (and by 2016 in non-euro area SEPA countries). customers can make cashless euro payments – via credit transfer and direct debit – to anywhere in the European Union, as well as a number of non-EU countries, in a fast, safe and efficient way, just like national payments. Source: ECB
TIPS	**TARGET Instant Payment Settlement (TIPS)** is a market infrastructure service launched by the Eurosystem in November 2018. It enables PSPs to offer fund transfers to their customers in real time and around the clock, every day of the year. Thanks to TIPS, individuals and firms can transfer money between each other within seconds, irrespective of the opening hours of their local bank. Source: ECB