Committee on Payments
and Market Infrastructures

BIS

CPMI Brief No 9

Safety and efficiency through payment pre-validation: spotting issues before money moves

Darren Chamberlain, Arif Ismail, Magnus Kroon, Thomas Lammer
and Peter Makgetsi

November 2025

www.bis.org
email@bis.org

Follow us

Safety and efficiency through payment pre-validation: spotting issues before money moves

Darren Chamberlain, Arif Ismail, Magnus Kroon, Thomas Lammer and Peter Makgetsi[1]

Highlights

- Payment pre-validation (PPV) enhances safety and efficiency by validating payment details before transactions are initiated. This process minimises errors, mitigates fraud risks and enhances compliance, while simultaneously improving user experience, trust and operational efficiency. The G20 South African Presidency and the Committee on Payments and Market Infrastructures (CPMI) also recognise the potential benefits of PPV.
- While PPV has demonstrated clear advantages for domestic payments, its adoption in cross-border contexts remains limited due to differences in legal, regulatory, technical and operational frameworks. Addressing these challenges is crucial to realising PPV's potential in enhancing cross-border payments.
- The success of PPV in cross-border payments hinges on the implementation of international standards and guidance to ensure interoperability across jurisdictions, strong governance frameworks, robust privacy safeguards and international collaboration. Furthermore, wider adoption will benefit from transparent pricing structures and consumer education initiatives.

Introduction

Identifying obstacles to the smooth and efficient processing of cross-border payments at an early stage increases the likelihood of resolving issues, assists in preventing financial crime and enhances the overall safety and efficiency of payments. Payment pre-validation (PPV) services are specifically designed to verify the accuracy, validity and completeness of payment information before initiating a cross-border payment. As a first step in the payment initiation, the payer provides the necessary details, which are then checked against the actual data. The payer proceeds only when a result is satisfactory, by confirming the payment and transferring the funds. These services help ensure that transactions meet all necessary technical, legal and regulatory requirements before processing, clearing and settlement. For instance, the confirmation of payee is a specific pre-validation service that authenticates the payee's information, typically based on at least a name and account identifier (such as an account number or a proxy like a phone number). This service is also referred to as verification of payee or beneficiary check.

[1] The authors thank Chakree Aksonthung, Holti Banka, Ulrich Bindseil, David Brown, Mark Choi, Antonio Perrella and Federico Semorile for their valuable comments and Fanni Leppanen for her excellent research assistance. Special thanks to Annah Masoga and the Policy and Regulation Division of SARB's NPSD for their invaluable support in organising and conducting the interviews. While this CPMI Brief has benefited from discussions and interviews with industry stakeholders, the Brief itself, as well as the views expressed therein, are those of the authors and do not necessarily reflect those of the organisations interviewed or their affiliates, the Bank for International Settlements (BIS), the CPMI or its member central banks.

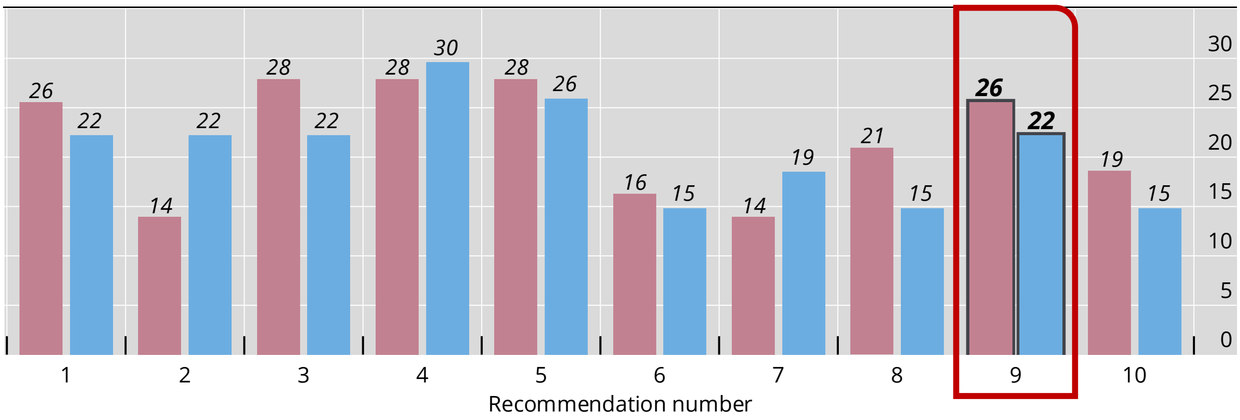
Pre-validation significantly improves the chances of successful payment execution while reducing costly rejections, returns and the need for manual interventions along the payment value chain. It also plays a critical role in mitigating fraud (eg authorised push payment (APP) fraud)[2] and non-compliance risks. Consequently, the widespread adoption of PPV services can help address many root causes of cross-border payment frictions, particularly those impacting the speed and transparency of such payments. Furthermore, pre-validation can also serve as a foundation for payment service providers (PSPs) to improve the user experience by displaying transfer costs, execution times and reporting requirements up front, thereby improving transparency.

An increasing number of fast payment schemes support pre-validation checks by PSPs. In some jurisdictions, PSPs are mandated to offer the confirmation of payee feature, whereas in others, its adoption is encouraged on a voluntary basis. While current pre-validation solutions primarily support domestic fast payments, their international rollout could significantly enhance cross-border payments. The CPMI's harmonisation recommendations for application programming interfaces (APIs) underscore the importance of interoperability among PPV solutions across jurisdictions (see Annex 2 and CPMI (2024a)).

Despite their benefits, the adoption of PPV services for cross-border payments has been limited. The fragmented global landscape for pre-validation services and their lack of interoperability are key factors contributing to this limited adoption. The CPMI report to the G20 on API harmonisation recommends that PSPs prioritise the development and harmonisation of pre-validation APIs to support the validation of essential data items within a payment request. API end users should, where available, utilise pre-validation services to reduce the likelihood of failure after initiation (CPMI (2024a)) (see Annex 2 for the full recommendation and potential action items).

CPMI API harmonisation recommendations considered to be most relevant

As a % of the FPS and RTGS system operators that already use APIs[1] Graph 1



Recommendation 1: open API standards; recommendation 2: existing harmonisation initiatives; recommendation 3: best practice design; recommendation 4: ISO 20022 and Financial Action Task Force recommendation 16 on payment transparency; recommendation 5: security; recommendation 6: common registries; recommendation 7: developer training and knowledge transfer; recommendation 8: developer resources; **recommendation 9: pre-validation;** recommendation 10: progress tracking and promoting adoption.

[1] Includes 43 FPS and 28 RTGS systems.

Sources: CPMI cross-border payments monitoring survey, 2025; BIS.

[2] PPV is one tool that can help mitigate payment fraud. This paper does not address other tools that can also contribute to the safe and efficient processing of cross-border payments.

According to the 2025 CPMI-Financial Stability Board (FSB) cross-border payments monitoring survey, fast payment system (FPS) and real-time gross settlement (RTGS) system operators regard the pre-validation recommendation as one of the most relevant measures to enhance cross-border payments (see Graph 1). In several jurisdictions, confirmation of payee is required by regulation (see Box 1).

Box 1

Regulatory requirements for confirmation of payee

The EU Instant Payments Regulation (IPR), adopted on 13 March 2024, aims to accelerate instant payments in the European Union for euro-denominated credit transfers. It amends the SEPA Regulation, the Cross-Border Payment Regulation, the Settlement Finality Directive (SFD) and the Payment Services Directive (PSD2). Under the IPR, PSPs offering standard credit transfers must also provide instant credit transfers. Charges for instant credit transfers cannot exceed those for standard credit transfers of the same type, ensuring cost equality. A key provision is the "verification of payee" service, which became mandatory in the euro area on 9 October 2025. It requires PSPs to verify the payee's details, such as their name and account information, before processing credit transfers. This service applies to both standard and instant credit transfers and must be offered free of charge to the payer, enhancing security and transparency. The regulation also mandates simplified sanctions screening, requiring PSPs to perform daily checks to ensure compliance with restrictive financial measures.

The National Payments Corporation of India (NPCI) has mandated that Unified Payments Interface (UPI) apps must display the exact PSP-registered names of recipients during transactions, effective 30 June 2025. UPI apps can no longer show customised or user-set names that differ from those in the PSP's records. Instead, the displayed name must match the official bank account holder's name without alterations. The NPCI initiative aims to enhance transparency and security in UPI transactions by ensuring that users can verify the recipient's identity before completing a payment.

In the United Kingdom, the UK Payment Systems Regulator (PSR) issued Specific Direction 10 in August 2019, requiring the six largest banking groups to implement confirmation of payee (CoP) by March 2020. These banks handle around 90% of Faster Payment System and CHAPS transactions. By July 2020, they had successfully implemented CoP, with some exemptions. To expand the CoP reach, the PSR issued Specific Direction 11 in February 2022 to transition CoP to a single technical environment (Phase 2), allowing more banks to adopt the service. Following a consultation in May 2022, the PSR directed around 400 additional financial firms to implement CoP, aiming to cover nearly all Faster Payment System and CHAPS transactions by October 2024.

Sources: ECB (2025); Kumar (2025); PSR (2025)

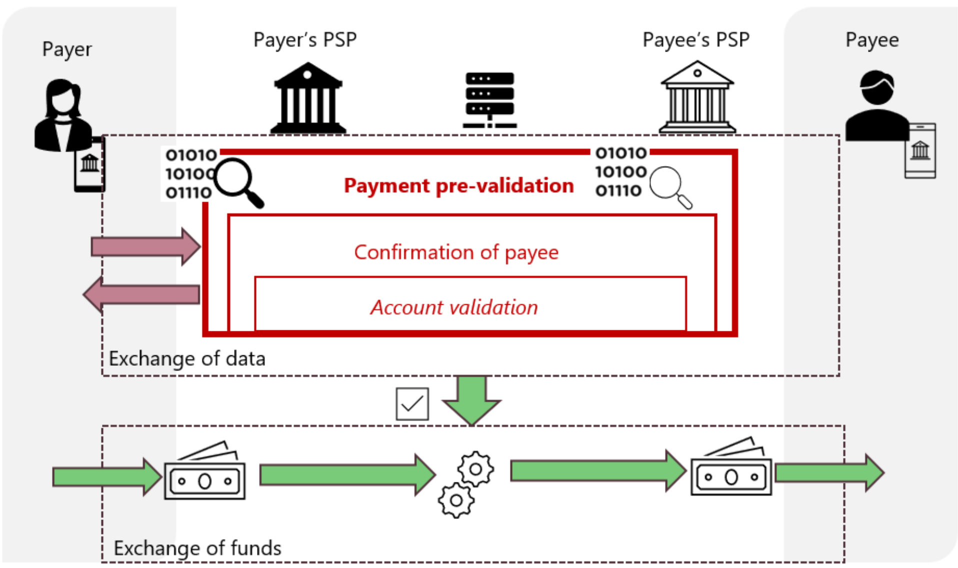
The G20 South African Presidency and the CPMI also recognise the potential benefits of PPV, which led the South African Reserve Bank (SARB) and the CPMI Secretariat to explore the opportunities and challenges associated with the international harmonisation and adoption of PPV services. The initial findings from a series of interviews with relevant stakeholders, including FPS operators, payments associations and solution providers, are laid out in this note. The G20-CPMI side event at the July Finance Ministers and Central Bank Governors (FMCBG) meetings and the flagship conference "Advancing cross-border payments – identifying opportunities and challenges for Sub-Saharan Africa" provided further valuable insights.[3]

This Brief aims to present selected preliminary considerations rather than draft guidance or best practices. Importantly, it focuses specifically on confirmation of payee as a dedicated feature of PPV. The considerations serve a dual purpose. First, they are intended to inform practitioners and authorities exploring the use of PPV. Second, they aim to provide a foundation for further dialogue and engagement with stakeholders. They are also expected to contribute to the work of the CPMI payments interoperability and extension (PIE) task force in 2026.

What is (new about) payment pre-validation?

The practice of PSPs verifying the payment information provided by their customers is not new. Since the introduction of structured payment messages and messaging standards, PSPs have employed syntactic checks to identify potential errors or missing information early in the payment process. However, PPV extends beyond these structural and format checks by validating the actual accuracy and completeness of the information (Graph 2).

High-level overview of the concept of payment pre-validation — Graph 2



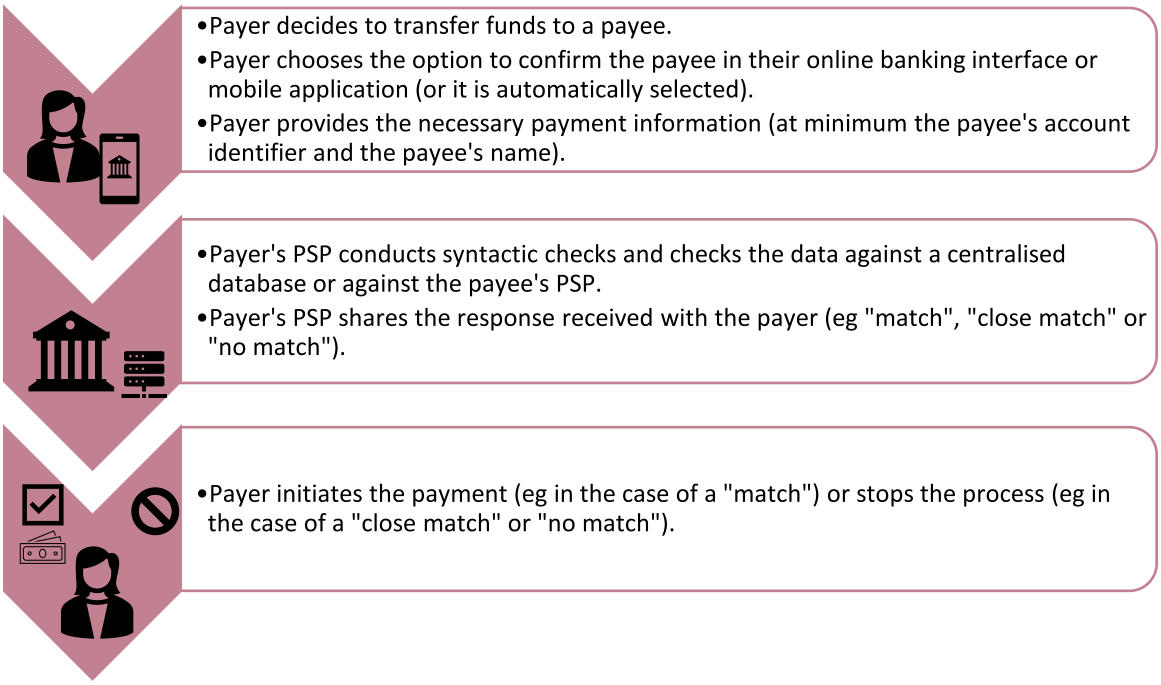
Source: Authors' illustration.

PPV can comprise several features, from account validation and confirmation of payee to additional quality checks verifying if the payment data include all information required by the target jurisdiction or PSPs. Account validation focuses on verifying if the beneficiary account exists and whether it is active or dormant, but not on whether the payee's name provided also matches the account owner's

[3] For more information on the FMCBG side event "Enhancing cross-border payments in sub-Saharan Africa" in Zimbali, KwaZulu-Natal, see the SARB website. Information on the conference "Advancing cross-border payments – identifying opportunities and challenges for Sub-Saharan Africa" in Pretoria in October 2025 can also be found on the SARB website.

name. Confirmation of payee focuses on confirming that the payee is the intended recipient of the funds. This is typically accomplished by matching the account identifier (eg account number or proxy identifier, such as a mobile phone number) and the payee's name, as provided by the payer, with the information stored in a central database or by the payee's PSP. This note primarily focuses on the confirmation of payee feature of PPV (Graph 3).

Simplified overview of the confirmation of payee feature — Graph 3



Source: Authors' illustration.

What promise does payment pre-validation bring?

PPV solutions are essential components of the financial crime prevention toolkit, though they are not standalone solutions for combating fraud. Confirmation of payee can significantly reduce credit transfer fraud, particularly APP fraud, where individuals are deceived into transferring funds to fraudulent (but plausible-sounding) accounts. Although credit transfer fraud is relatively lower than card payment fraud in proportional terms, it can surpass card fraud in absolute losses. For example, despite a 14% year-on-year decrease, fraudulent credit transfers originating from PSPs in the European Economic Area and received worldwide amounted to EUR 1.131 billion in the first half of 2023 alone (EBA and ECB (2024)).[4]

[4] These fraudulent activities resulted in EUR 967 million in losses for credit transfers in the European Economic Area during the same period, with end users bearing the vast majority (86%). Of these losses, 43% of the total value and 36% of the volume of fraudulent credit transfers were linked to cross-border payments (EBA and ECB (2024)).

While comprehensive data on fraud reduction attributed to PPV solutions are limited, these solutions are widely regarded as effective safeguards against misdirected funds, fostering trust in digital payments. This is particularly important for fast payments, which are irrevocable once processed. In the United Kingdom, certain types of end user fraud losses have declined by 20-40% since the introduction of confirmation of payee (Pay.UK (2025b)). In 2024, overall APP fraud losses decreased by 2% to just over GBP 450 million, while the number of cases fell by a more significant 20% – the lowest figures for both cases and losses since 2021. UK Finance attributes these declines to collective efforts, including confirmation of payee (UK Finance (2025)). However, global APP fraud losses are projected to increase by 12% annually, from nearly USD 4.4 billion in 2023 to over USD 7.6 billion in 2028 (ACI Worldwide and GlobalData (2024)).[5]

PPV solutions are not standalone fraud prevention measures. User education is critical to addressing social engineering attacks and other fraud types that technology alone cannot mitigate. Providing immediate feedback on payment details, expected transaction times and charges can enhance end user satisfaction and build trust. Confirming the beneficiary's identity can particularly boost trust in digital payments among newly banked and underbanked populations or individuals previously targeted by APP fraud. This, in turn, supports financial inclusion by making payment services more accessible and reliable, thereby encouraging the use of digital payments by those with financial access.

Misdirected, rejected or returned payments caused by human error or incomplete information increase the need for manual intervention, leading to costly exception handling. Globally, payment executives report that 14% of cross-border payments are not automatically completed and incur charges from PSPs. The average global fee for a rejected or repaired payment is USD 12. Issues with beneficiary name and address details (21%) and the use of non-IBAN account identifiers (15%) are the primary reasons for failed payments. Manual checks of beneficiary details are still conducted by 72% of respondents, creating friction and operational inefficiencies in payment processes (LexisNexis (2023)).

The confirmation of payee feature helps prevent payments from being sent to incorrect accounts due to human error when entering payee details. It flags mismatches, allowing payers to correct details before initiating payments. By reducing operational overhead and improving data quality, PPV solutions enhance automation and straight-through processing, leading to greater efficiency and lower costs in both domestic and cross-border payments (World Bank (2025)). Since the UK Faster Payment System launched its confirmation of payee service in 2020, it has seen a 59% reduction in credit recovery requests sent to beneficiary banks (Pay.UK (2025b)).

PPV also supports compliance with international anti-money laundering and countering the financing of terrorism (AML/CFT) standards. Notably, the Financial Action Task Force (FATF) has revised recommendation 16 on payment transparency, introducing alignment check obligations. These include post-validation checks, holistic ongoing monitoring and pre-validation checks (such as confirmation of payee) (FATF (2025)).

[5] The proportion of real-time payments contributing to overall APP fraud losses is expected to rise from 63% (USD 2,773 million) in 2023 to 80% (USD 6,106 million) in 2028, representing an increase of over USD 3.3 billion (ACI Worldwide and GlobalData (2024)).

What are key decisions for the design and rollout of payment pre-validation services?

Message formats and information exchange

The current PPV landscape reflects no clear preference between tailored API-based solutions and traditional messaging networks or standards. While some jurisdictions have embraced API-based solutions to implement PPV services, others rely on traditional messaging standards, often leveraging ISO 20022. Confirmation of payee involves two critical ISO 20022 messages: the identification verification request (acmt.023) and the identification verification report (acmt.024). The acmt.023 enables a payer to confirm a payee's details before initiating a fast payment, while the acmt.024 provides a response to this request (World Bank (2025)).

The type of information exchanged varies across implementations and is shaped by user preferences, data privacy laws and regulations. Common practices, such as partial or masked disclosure and encrypted communication channels, have proven effective in multiple jurisdictions, safeguarding sensitive data and avoiding the unnecessary disclosure of personal details. For example, in some jurisdictions, the correct name is displayed in clear text for verification as part of the confirmation of payee, while in others, the name is either masked or not provided at all. In such cases, the response may be standardised with outcomes such as "match", "close match" or "no match." These latter approaches adhere to data minimisation principles, ensuring that only the information strictly necessary for validation is disclosed (World Bank (2025)).

To meet the speed requirements of fast payments, PPV responses typically take only a few seconds. Depending on local payment practices, PPV solutions process multiple account identifiers, including proxy identifiers such as account numbers, IBANs, national identity numbers, mobile phone numbers and email addresses. This ensures relevance across diverse payment channels and, in some cases, across jurisdictions. The type of information processed and the service-level requirements, such as speed, will ultimately shape the operational design of the PPV solution.

Operational design

PPV implementations can follow centralised, decentralised or hybrid data management models. In decentralised systems, data are stored and maintained by the information "owner", typically the PSP where the payee holds their account. When a payer requests verification, the request is sent to the payee's PSP, which compares it with its database. In centralised systems, information owners update a central database in real time or near real time. PPV requests are then processed within this central database, which is often managed by the FPS operator. This approach may also incorporate a centralised proxy directory service that links account numbers with other identifiers – most commonly mobile phone numbers. Hybrid models combine features of both centralised and decentralised systems, depending on the capabilities of the responding PSP (World Bank (2025)).

The choice between decentralised and centralised data management models involves trade-offs (Table 1). A decentralised approach, where data remain with individual PSPs, can enhance privacy and minimise the risks associated with a single point of failure. However, it may also increase complexity in maintaining consistent data quality and interoperability. Conversely, a centralised model offers streamlined data access and uniformity but may raise concerns about data security, timeliness, privacy and compliance with jurisdiction-specific regulations. Successfully balancing these considerations, alongside implementing encryption and data masking, is essential for designing data management systems that effectively support both domestic and cross-border PPV implementations.

Comparing centralised and decentralised models — Table 1

Model	Pros	Cons
Centralised	• Simplified data management: Updates and management are easier with all data in one location. • Consistency: Uniform verification process reduces discrepancies across PSPs. • Faster verification: Streamlined processes enhance transaction speed and user experience. • Easier compliance: Central oversight simplifies regulatory adherence.	• Single point of failure: System failure could disrupt all users and PSPs. • Privacy concerns: Centralised storage raises risks of unauthorised access and data breaches. • Dependency on central authority: Reliance on one entity may slow responsiveness to issues.
Decentralised	• Enhanced security: Storing data with individual PSPs reduces risks of a single point of failure. • Flexibility: Participants can customise processes to suit their needs and customer base. • Wider participation: Broader involvement improves efficiency and reach. • Local data control: PSPs manage their own data, enhancing trust and accountability.	• Inconsistency: Variations in data management across PSPs may cause discrepancies in verification. • Complex integration: Coordination between participants complicates implementation. • Slower verification: Network-based processes may result in longer verification times. • Regulatory challenges: Compliance across diverse participants can be more difficult to manage.

Source: World Bank (2025).

Governance, participation and access

Governance defines the decision-making processes and authority within the PPV solution, as well as the accountability and responsibilities of operators and participants, including liability allocation and compliance obligations. Key considerations for operators when developing and implementing a governance approach for payment-related arrangements include compliance with legal and oversight requirements, ownership and operational structure, the type of governing body and stakeholder engagement (including public-private sector collaboration) (CPMI (2024b)). Effective governance provides legal certainty, fosters trust among participants and establishes a foundation for international cooperation, enabling smoother cross-border adoption of PPV solutions.

Typically, governance frameworks are grounded in a comprehensive rulebook and supported by mechanisms to monitor performance and enforce participation.[6] Effective governance should also ensure compliance with AML/CFT requirements, especially FATF recommendation 16 on payment transparency. Governance frameworks must align with jurisdictional data protection regulations, to safeguard privacy and ensure legal compliance.

[6] Examples for publicly available rulebooks are the Single Euro Payments Area *Verification of payee scheme rulebook* and the Nordic Payments Council *Confirmation of payee scheme rulebook*.

Participation rules, enforced through scheme governance, provide legal certainty and establish accountability for all stakeholders. Participation in and use of PPV solutions is often contingent on participation in the FPS itself. PPV solutions aim to balance inclusivity with the need to prevent inappropriate use of the service. Strong know-your-customer (KYC) practices are fundamental to delivering reliable PPV services, ensuring that all participants meet the necessary security and compliance standards. Broad participation by both bank and non-bank PSPs is a key success factor for any PPV solution and may even be mandatory for PSPs within a scheme.

Eligibility for participation is typically based on adherence to technical, security and KYC standards. For cross-border adoption, access and participation rules must also align with international frameworks to address differing legal, privacy and regulatory regimes. This includes implementing secure data-sharing arrangements, addressing data residency requirements and ensuring KYC practices are robust enough to support cross-jurisdictional transactions. By fostering universal access, enforcing stringent eligibility criteria and ensuring cross-border compatibility, PPV services can achieve both inclusivity and integrity. This approach not only supports domestic adoption but also lays the groundwork for seamless global implementation, enabling PPV to function as a reliable and scalable solution across jurisdictions.

Experience across jurisdictions demonstrates that the adoption of PPV solutions is most effective when participation is mandated by regulation or scheme rules, ensuring consistency and broad coverage. Voluntary or commercially driven participation can result in slower uptake and uneven coverage, thereby limiting the potential benefits. Mandatory adoption may promote comprehensive rollout and stronger network effects. For instance, in the United Kingdom, the high adoption rate is likely attributable to the Payment Systems Regulator's directive in October 2022, which mandated PSPs to implement the service by 31 October 2024 (Pay.UK (2025a, 2025b)).[7] Adoption is further facilitated by standardised onboarding and adherence procedures, which reduce integration barriers, and by extending participation to non-bank PSPs and corporations, thereby enhancing network effects.

Legal and regulatory compliance

A significant challenge for PPV solutions, particularly those operating across jurisdictions, lies in navigating diverse legal and regulatory frameworks. Issues such as liability allocation, AML/CFT obligations and varying data protection and privacy regimes often present more substantial barriers than technical challenges. Uncertainty around liability in cases of misdirected or fraudulent payments can discourage participation, while data localisation rules and consent requirements complicate the exchange of information across borders. Robust authentication and authorisation protocols, along with secure data-sharing arrangements between jurisdictions, can facilitate cross-border adoption. Additionally, ongoing monitoring and maintenance are essential for adapting to evolving regulatory and operational requirements.

Economic model

An appropriate economic model is critical to ensuring the sustainability and scalability of PPV solutions. The cost recovery model is the most widely used approach. For economic sustainability, PPV solutions must at least recover their costs through fee arrangements. In many fast payment schemes, charges are integrated into broader transaction or service charges rather than treated as standalone fees, providing

7 In the United Kingdom, the service is offered by nearly 400 PSPs, covering more than 99% of all payments processed through the Faster Payment System, Bacs Payment System and CHAPS. The number of checks increased from 14,000 per month in June 2020 to over 70 million per month by July 2025, averaging 26 checks every second.

PSPs with greater cost predictability. Regulatory or scheme mandates can also act as indirect incentives making participation in PPV solutions a condition for accessing FPS.

PSPs are typically charged either an annual fee or a pay-per-use fee. Generally, when confirmation of payee services are mandatory, they are not charged directly to the end user. However, when these services are positioned as value-added offerings, end users might also be charged direct fees (World Bank (2025)). Transparent and predictable pricing models may promote adoption and scalability.

Usability, awareness and financial education

Usability, education and awareness are critical enablers for the successful adoption of PPV. Especially if used for fast payments, it is important that PPV upholds efficient processes and strives for real-time results. In the case of negative outcomes, users might find visual alerts or advice on the preferred course of action useful (eg not to authorise the payment but verify and correct the payment information). Particular consideration in designing and implementing PPV may be required for individuals with additional needs such as those with sight impairments or dyslexia, older adults and other groups that may face higher risks (Pay.UK (2018)).

By educating end users, participants can strengthen trust and encourage broader use. Coordinated consumer education campaigns are particularly important in enabling users to correctly interpret mismatch warnings, reinforcing confidence in the service. These efforts should align with broader financial literacy initiatives and complement fraud-prevention policies, ensuring a consistent approach to user engagement.

Education campaigns also play a direct role in promoting adoption and reducing fraud. Informed users are less likely to initiate authorisation of the payment if the confirmation of payee response is a close or no match, to avoid misdirected payments and to prevent social engineering and APP fraud attempts. By enhancing understanding of how PPV functions and the protections it offers, education strengthens user confidence in digital payments and contributes to reducing fraud-related losses. This, in turn, reinforces the effectiveness of PPV solutions and supports their wider adoption (Pay.UK (2018)).

What challenges lie ahead for broader (cross-border) use of payment pre-validation?

Cross-border use cases are not yet the primary focus for most PPV solutions, which generally prioritise domestic rollouts. Few are actively exploring cross-border linkages at this time. Hence, the cross-border application of pre-validation remains in its early stages. This reflects the inherent complexity of aligning technical, operational and governance frameworks across jurisdictions. Bilateral interlinking or regional payment integration initiatives present opportunities for cross-border adoption. However, aligning technical, operational and governance frameworks across jurisdictions remains a significant challenge.

Even at the domestic level, participation in and use of PPV often depend on external factors, such as rising fraud rates or regulatory requirements mandating the service. Without stronger international coordination, diverse implementations may lead to future harmonisation challenges. The CPMI's harmonised ISO 20022 data requirements and API recommendations could encourage the use of internationally recognised identifiers and standardised data formats for PPV. Developing a cross-border PPV data model could further strengthen cross-border interoperability and enhance efficiency and scalability.

A wide variety of operational models and business use cases are currently being employed or rolled out, tailored to the specific needs of individual jurisdictions. These variations reflect differences in regulatory environments, market structures and user preferences. Many stakeholders highlighted that the algorithm and tolerance levels determining the outcome of confirmation of payee checks must account for jurisdiction-specific naming practices, including the use of middle names, abbreviations, special characters, generational suffixes and even call names. The algorithm and tolerance levels are crucial design elements for minimising false negatives while ensuring a high level of accuracy.

Internationally agreed harmonisation recommendations specific to PPV could form a first step for cross-border interoperability. Aligning with harmonised ISO 20022 data requirements and converging on common API specifications ensure that domestic systems remain interoperable with regional and cross-border frameworks.

The success of PPV depends not only on technical interoperability but also on effective governance, supportive legal and regulatory frameworks and end user adoption. Many stakeholders perceive governance challenges, such as coordinating among multiple parties, as more significant than technical interoperability challenges. Effective governance structures are essential and must align with existing legal frameworks (eg AML/CFT, data protection), which are unlikely to change in the short term.[8] Awareness and financial education campaigns are also critical to driving end user adoption.

Although legal and regulatory differences are challenging in their own right, data privacy compliance emerged as a major concern during stakeholder interviews. The success of these services relies on striking a delicate balance: providing sufficient information for meaningful validation while ensuring the protection of personal data. To address this, many jurisdictions have adopted measures such as name masking, partial disclosure of identifiers and encrypted communication channels. These practices are essential not only for complying with national data protection laws but also for building user trust, as individuals are more likely to embrace PPV when reassured that their personal information is secure. However, while domestic solutions have successfully navigated these challenges within their respective legal frameworks, implementing PPV – particularly confirmation of payee – across borders introduces significant complexities. Variations in privacy laws, consent requirements and liability frameworks create substantial barriers to achieving cross-border interoperability.

Conclusions and next steps

PPV has emerged as a promising tool to enhance trust, reduce errors and improve the efficiency of payments. Domestic implementations demonstrate clear benefits, including reducing misdirected payments, supporting fraud prevention and boosting user confidence. However, cross-border use remains in its infancy, with significant challenges related to legal frameworks, data protection, governance and interoperability.

CPMI stakeholder engagement groups could play a role in overcoming some of the challenges associated with cross-border PPV. To address these challenges and capitalise on the opportunities identified in the (cross-border) rollout of PPV solutions, several potential pathways could be explored. These options aim to align with existing frameworks, foster collaboration among stakeholders and advance global standardisation efforts.

8 Similar challenges can be observed when it comes to interlinking FPS. Hence, the CPMI issued recommendations on governance and oversight for the interlinking of FPS to provide guidance in this regard (CPMI (2024b)).

Strengthening alignment with and leveraging of CPMI frameworks

Exploring closer alignment with existing CPMI frameworks and recommendations – such as those on API harmonisation and ISO 20022 arrangements – could help address many of the identified challenges. This could involve leveraging CPMI frameworks and recommendations to promote PPV solutions, particularly confirmation of payee, on a global scale. The technical interoperability challenges highlighted during the interviews suggest that greater emphasis could be placed on promoting the CPMI's harmonised ISO 20022 and API requirements. This includes adopting internationally recognised identifiers and standardised data formats, which are essential for improving interoperability across jurisdictions.

Facilitating experience sharing through CPMI stakeholder groups

Providing a platform for sharing experiences and best practices related to PPV solutions could raise awareness of this topic among both public and private sector participants, foster collaboration and accelerate progress. This initiative could be coordinated under the CPMI's community of practice on payment systems (CoPS) and the PIE task force, leveraging their existing structures to encourage knowledge exchange among stakeholders. In line with its objectives of promoting API use, the PIE task force could play a pivotal role in fostering interoperability and driving harmonisation across solutions, addressing key challenges in the PPV ecosystem and promoting more cohesive global adoption.

Seeking additional insights on PPV

The CPMI Secretariat seeks further insights from a broad set of stakeholders on the interview questions (Annex 3), which could feed into the work of the stakeholder groups. Responses to the questions and comments on this Brief are welcome **by the end of January 2026**. Send responses to the CPMI Secretariat (cpmi@bis.org) with "Payment pre-validation" in the subject line. Responses will be shared with CoPS and PIE task force and can also be published on the BIS CPMI website. The BIS reserves the right not to publish submissions. Commercial or other sensitive information should not be included in the submissions, or they may be included with redactions for distribution and publication clearly noted.

References

ACI Worldwide and GlobalData (2024): *2024 scamscope: the battle for trust. APP scam trends in the U.S., the U.K., Australia, India, Brazil, and the UAE.*

Committee on Payments and Market Infrastructures (CPMI) (2024a): "Promoting the harmonisation of application programming interfaces to enhance cross-border payments: recommendations and toolkit", *CPMI Papers*, October.

——— (2024b): *Linking fast payment systems across borders: governance and oversight – final report to the G20*, October.

European Banking Authority (EBA) and European Central Bank (ECB) (2024): *2024 report on payment fraud*, August.

European Central Bank (ECB) (2025): "Instant Payments Regulation".

Financial Action Task Force (FATF) (2025): "FATF updates standards on recommendation 16 on payment transparency", 18 June.

Kumar, A (2025): "No more scams: UPI apps to now show recipients' bank-registered names only", *Business Standard,* 26 May.

LexisNexis Risk Solutions (2023): *True impact of failed payments*, February.

Pay.UK (2018): *Confirmation of Payee: understanding consumer and stakeholder perspectives*, October.

——— (2025a): "Confirmation of Payee: the journey so far", 6 June.

——— (2025b): "Pay.UK discusses the evolution of Confirmation of Payee with Tell.money", 29 August.

Payment Systems Regulator (PSR) (2025): "Confirmation of Payee".

UK Finance (2025): *Annual fraud report 2025.*

World Bank (2025): *Prominent overlay services in fast payment systems: request to pay and confirmation of payee*, September.

Annex 1: List of interview partners

Stakeholders interviewed

Table A1

Australian Payments Plus	PayInc (formerly BankservAfrica)
Banfico	Pay.UK
CBI Globe	Pix
Confirm by Kinexys Liink	Sarie
Dutch Payments Association	Surepay
European Payments Council (EPC)	Swift
Iberpay	United Payments Interface (UPI)
iPiD	

Annex 2: CPMI API harmonisation recommendation on pre-validation

Recommendation 9: Pre-validation PSPs should prioritise the development and harmonisation of pre-validation APIs that support the validation of key data items within a payment request. API end users should, where available, make use of pre-validation services to reduce the likelihood of failure after initiation.

Pre-validation is designed to verify that details of a cross-border payment are correct before processing begins so that the payment can be processed efficiently without automation breaks. Pre-validation can also ensure that the payer is aware of the terms of the transaction (fees, foreign exchange (FX) rates, predicted time of delivery) before committing to its execution. Standardised APIs are well adapted to the requirements of pre-validation services, which require real-time request/response interactions, and may need to aggregate data from multiple implementations to satisfy a request.

Pre-validation checks include confirmation of payee, ie checking that the payee’s account exists and is open to receive funds, how long the payee’s account has existed and also that the name of the account owner matches that of the party the payer wishes to pay. Other elements that can be checked or determined include purpose codes (whether these are required for the destination market, and if so whether an appropriate code has been provided), clearing codes, market infrastructure amount limits and/or operating hours, FX rates and fees, and estimated delivery time.

Potential action items:

1. PSPs should prioritise development of APIs that enable transparency for end users on fees, FX rates and delivery time, and check that key details of the payment (such as the creditor account) are correct before processing begins.
2. PSPs that offer payment services to end users should take advantage of pre-validation APIs to provide the highest levels of transparency and processing efficiency.
3. Standards organisations should prioritise development of standards for pre-validation APIs, recognising that pre-validation requests may be satisfied by combining data from multiple services and that standardisation is key to making this safe and efficient.
4. In jurisdictions where confirmation of payee services are available for domestic payments, providers of these services should work to extend them to financial institutions and PSPs in originating countries to cater to cross-border payments via pre-validation APIs. These APIs should take into account jurisdictional limitations with respect to payee privacy and security.
5. In jurisdictions where confirmation of payee services do not exist, authorities, payment system operators and standards organisations should encourage the creation of such a service for domestic and cross-border payments via public-private collaboration. This service should be developed and implemented in an open and neutral manner so as not to disadvantage any stakeholders within a given jurisdiction.

Annex 3: Interview questions

Overview

1. Please provide an overview of your payment pre-validation solution, focusing on the confirmation of payee, covering the following aspects:
    a. Basic functioning and use cases: Describe how the solution works and type of payments covered.
    b. Governance: Explain the governance framework overseeing the solution.
    c. Business model and motivations: Outline the business model and other driving factors such regulatory requirements and cost savings from lower rates of rejects/returns.
    d. Timeline: Provide a timeline for the development and implementation of the solution.
    e. Partners: Identify key partners involved in the solution.
    f. (Target) Markets: Specify the target markets for the solution.

Technical and operational specifications and challenges

2. Are you using any specific financial messaging or API standards for your solution? If so, which standards are those and what considerations influenced your choice?
3. What technical or operational challenges have you faced in the rollout and adoption of pre-validation/confirmation of payee among financial institutions?
4. What is the capacity of your solution to scale, to handle high volumes of transactions and/or support additional payment service providers?
5. What security protocols are used by your solution to ensure security of data/transactions and fraud prevention, and what security challenges have you faced in implementing your solution?
6. How do you maintain up-to-date payee information (eg leveraging or maintaining directory lookup services)?

Interoperability and harmonisation

7. In your opinion, what are or would be the biggest challenges in cross-border interoperability for your solution (eg data frameworks, cyber resilience)?
8. What challenges have you encountered in ensuring interoperability across different financial institutions?

End user and market dynamics

9. Has the rollout been accompanied by end user awareness or education campaigns? How has the offering of pre-validation/confirmation of payee been received by end users (consumers and businesses)?
10. What challenges have emerged, if any? Have there been any notable behavioural changes in how end users initiate payments?
11. What factors influenced the selection of data to be provided by/information displayed to the payer?

Regulatory and legal challenges

12. What regulatory or legal challenges (including regulatory or legal differences across jurisdictions) did you face in designing and rolling out your pre-validation/confirmation of payee solution (eg data privacy/protection laws)?

13. To what extent can your solution support financial institutions' compliance with the revised FATF recommendation 16 on payment transparency?

Conclusion

14. Do you have any further thoughts or additional insights on how we can collectively work towards greater harmonisation and interoperability of such solutions (including the role of international bodies such as technical standard setters, international organisations and standard-setting bodies)?

Bank for International Settlements (BIS)

ISSN (online) 2958-8758
ISBN (online) 978-92-9259-892-1