ENHANCING CROSS-BORDER PAYMENTS: ADDRESSING FRAUD

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 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

Detecting and preventing fraud has become a major priority in the context of fast payments (also referred to as instant payments), particularly in the cross-border space. This paper by members of Payments Interoperability and Extension (PIE) Task Team 2 identifies several critical challenges and provides key considerations to enhance fraud prevention measures from an industry perspective.

The key considerations have ambitious goals: a less aspiring approach would lack clarity of vision, pace, and direction. They are addressed to public bodies and the private sector, payment system operators and owners, banks and non-bank payment service providers (PSPs). Taking the key considerations forward will require collaboration and coordination. Specifically, detailed work will be required to ensure a pragmatic, sequenced, and proportionate approach that considers competing priorities, is evaluated for unintended consequences, and is supported by analysis and consultation. International collaboration is fundamental; therefore international coordinating bodies such as the Financial Stability Board (FSB) and the Committee on Payments and Market Infrastructures (CPMI) are in the view of the PIE Task Team well-positioned to play a central role.

Combating fraud in the context of cross-border payments is essential.

With the rapid growth of cross-border payments and the evolving nature of fraud, specifically the rise of authorised push payment (APP) scam fraud, there is a need for a focused and targeted response to ensure safety and security of payment flows. However, addressing fraud within the cross-border payments landscape is challenging.

The main challenges include: (i) data fragmentation, which creates difficulties in accessing complete transaction data across different payment networks; (ii) insufficient development of enabling infrastructure and operational capabilities, which limits the ability of payment systems to support real-time processing. This includes outdated legacy systems, lack of automation in pre-transaction checks, and inadequate fraud prevention mechanisms that struggle to operate within compressed transaction windows; (iii) immature pre-validation solutions, which lack the capability to effectively implement pre-validation of beneficiaries and payment routes.

Data fragmentation is further exacerbated by different privacy laws and regulatory frameworks, which mean that PSPs cannot easily share data across borders, thereby hindering the establishment of a common, real-time fraud registry interoperation across FPS. As a result, fraudsters and mule accounts cannot be tracked across borders and the cross-border recovery of funds for customers becomes more challenging.

KEY CONSIDERATIONS AND ACTIONS FOR INDUSTRY

1. Payment networks and FPS operators seek to establish interoperable fraud registries.

- Establish interoperable fraud registries, and enable their interoperability with existing fraud registries where possible, to improve the identification of known fraud perpetrators and mule accounts, and to enhance overall fraud prevention, with a view to transitioning to interoperability of real-time fraud registries as a further step.

2. Payment networks and FPS operators seek to leverage technology for enhanced data sharing.

- Develop mechanisms for compliance with the recently updated FATF Recommendation 16 on payment transparency for data visibility across payment networks.
- While full transparency may not be compatible with privacy/confidentiality restrictions, new privacy-enhancing technologies (PETs), such as tokenisation, can provide valuable capabilities to support data sharing and should be further explored.
- At the same time, exploring ways how to allow for full transparency should continue as the final objective.

3. FPS operators and PSPs implement robust pre-validation processes.

- Set up systems that support pre-validation and testing of payment routes.
- Ensure transactions are thoroughly vetted before execution to enhance security.
- A shared data model and common set of standards should be considered to reduce fragmentation and eliminate gaps exploited by fraud networks.
- Ensure robust fraud mitigation and risk management is 'built-in' by design, incorporating fraud risk management practices in scheme rules and ensuring compliance with these.

4. PSPs work collaboratively to share KYC best practices with peers globally and adopt leading KYC practices.

- PSPs should share information on the most effective practices for the detection of fraud perpetrators and mule accounts, such as those provided by the Wolfsberg Group or ISO 37003.
- Extending KYC into "Know Your Customer's Customer" (KYCC) can provide deeper insights into the potential risks and enhance the overall prevention efforts and should therefore be explored.
- International standard setters should act as a central point to support the promotion of mutually agreed KYC standards across jurisdictions.

5. Industry participants leverage advanced technologies for fraud detection, shaped by their role in the ecosystem.

- Continue to integrate advanced technologies, particularly artificial intelligence (AI), into fraud detection processes to identify anomalies and enhance fraud prevention capabilities.

- PSPs should take into account that the applications of AI will depend on the role and activity of each PSP provides (eg beneficiary PSPs focusing on mule account detection).

6. Industry associations and international standard setters foster industry collaboration and regulatory alignment.

- Encourage collaboration among industry stakeholders to facilitate the sharing of best practices and address common challenges.
- Develop and submit structured, validated input, such as technical standards, risk indicators, and operational data, to support authorities in creating consistent legal frameworks for data sharing and interoperable trust models.
- Recognise and address institutional barriers to collaboration, including legal constraints and reputational risks, by proposing governance models and incentives that encourage meaningful participation.

KEY CONSIDERATIONS AND ACTIONS FOR PUBLIC SECTOR

1. International standard setting bodies and operators of cross-border payment systems act as a catalyst for the adoption of universally accepted definitions for fraud.

- Given the significant opportunity for the public and private sectors to collaborate in establishing universally accepted definitions that institutions can rely on, public authorities should consider initiating the necessary dialogue.
- This collaboration should be organised such as to provide a foundation for implementation of standard practices globally, thereby enhancing the overall security of cross-border payment systems.

2. Regulators globally consider implementing regulations to allow PSPs to effectively intervene in fraudulent activities.

- This could include the granting of safe harbours and PSP interventions, such as pausing transactions on suspicion of fraud, without liability to their clients:
- The impact of these initiatives would be maximised if led by local regulators and if it aimed at coordinating the industry towards a more favourable outcome.

3. Legislators bring all parties into a regulatory framework to ensure appropriate actions are taken.

- More analysis could be undertaken about where fraud typically originates, eg through featuring fraudulent communications and advertisements, including eg telecommunications companies (telcos), social media companies, internet service providers, and fintechs.
- Public authorities could arbitrate these efforts, ensuring a coordinated and comprehensive response. All parties need to be brought into a framework that sets the right incentives and engages them to take steps to prevent abuse of their infrastructure or services.

4. Regulators consider options for legislation to support the establishment of central fraud repositories/exchanges.

- The experience of countries with advanced FPS, where authorities have successfully established central repositories/exchanges for fraud, could be studied to identify key success factors.
- AML frameworks which contain a "tipping-off" provision that restricts the sharing of information indicating a suspicious transaction could be revisited and adjusted (where necessary) to allow for the sharing of information with fraud repositories/exchanges, including those operated by the private sector.
- The implementation of such systems should be viewed as a first step in the journey towards effective real-time information sharing.

5. Legislators enable the private sector to deliver effective fraud mitigating solutions.

- The public sector should consider recognising new models proposed by the private sector, thereby allowing the private sector to develop innovative and effective solutions.
- Authorities could consider also the potential risk that actions of individual firms pose to the system to ensure that the approach is proportionate to this risk and that there is sufficient accountability across the different market players.

6. Central authorities encourage the implementation of digital identity.

- Encourage the implementation of advanced digital identity solutions to reduce identity theft and impersonation.
- Ensure that these advanced solutions make it harder for fraudsters to create fake identities or use stolen credentials, thereby increasing customer protection, and ensure that they enable PSPs to authenticate themselves and their communications to their clients, reducing bank impersonation fraud.

7. Authorities and private sector entities invest in consumer education and improve financial literacy.

- Through increased education and awareness about the sources of fraudulent activity, individuals should be better equipped to identify red flags and make informed financial decisions. This should also reduce the likelihood of falling victim to fraud or scams.

8. Strengthen transnational law enforcement and inter-agency collaboration.

- Transnational law enforcement and inter-agency partners are encouraged to prioritise the development of real-time intelligence-sharing frameworks, coordinated investigations, and joint operational hubs that bring together financial institutions, telecoms, fintechs, and cybercrime units.
- Successful transnational models, which have demonstrated the benefits of such collaboration, should be studied to identify best practices and key success factors.

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 cross-border payments programme. 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 stocktakes and analysis. As the programme has turned to implementation, the Bank for International Settlements' 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-led Cross-Border Payments Interoperability and Extension (PIE) task force's primary focus is to strengthen private sector participation in pursuing the key objectives of the G20 cross-border payments programme. In the first phase (2023 to the beginning of 2025), the PIE task force comprised around 30 representatives from industry associations, financial infrastructures, and PSPs, covering a wide range of business models and geographic areas. During this phase, 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).

This report has been drafted by Task Team 2 of the PIE task force and focuses on addressing fraud in fast payments, particularly from a cross-border payments perspective. The inputs for this report have been collected over the course of four workshops with Task Team 2 members, alongside analysis of relevant international case studies and external expert inputs. The rest of the report is structured as follows: Section 2 defines the current state; Section 3 provides an overview of benchmarking against best practices; Section 4 discusses the key considerations for the industry; Section 5 outlines the public sector support required to deliver these outcomes; and Section 6 concludes.

2. WHAT IS THE CURRENT STATE?

2.1. Barriers to address fraud in cross border payments

Detecting and preventing fraud has become a major issue in payments, particularly in the cross-border space. Cross-border payments are even more vulnerable to fraud than domestic payments. This can be illustrated, for example, by the fact that, in Europe in 2023, 71% of card payment fraud was linked to cross-border payments (EBA (2024)). Similar instances of fraud have been observed in other jurisdictions globally. It is therefore important to analyse and address fraud in cross-border fast payments at an early stage, before the volume of such payments becomes significant.

One significant challenge is the difficulty in accessing complete transaction data when two different payment networks are involved. This lack of data visibility hinders effective fraud detection, as fragmented information makes it challenging to track and analyse transactions comprehensively. System preparedness is another critical issue. Many jurisdictions lack targeted fraud mitigation measures for fast payments. While numerous fraud prevention measures are implemented during and after payments, pre-transaction checks are still in the early stages of development. This early stage of pre-checks often leads to false positives and false negatives, causing unnecessary delays and complications.

The need for pre-validation of beneficiaries and testing of payment routes, as well as the implementation of tokenisation, to securely handle sensitive information by replacing it with a non-sensitive

"token," is widely recognised. However, current systems are often not yet set up to accommodate these processes effectively. This gap in pre-validation and tokenisation capabilities leaves transactions vulnerable to fraud at the initial stages. Establishing thresholds and structured payment methods is necessary to recognise when transactions are at risk of failure. Transaction risk indicators could aid in identifying fraudulent activities. Additionally, the use of artificial intelligence (AI) in the processing chain could be enhanced to help identify anomalies and improve fraud detection.

The absence of a common means of fraud registry interoperation across FPS creates a challenge for data sharing across jurisdictions. Fraud registries are centralised databases containing information about known fraudsters and their most common methods of committing fraud. Interoperability for such registries would enable the identification of known fraudsters, enhancing the ability to prevent fraudulent activities. Collaboration between institutions is paramount, and lessons could be learned from telcos, which share fraudulent mobile numbers and KYC data between providers. Additionally, challenges in sharing intelligence about fraudsters, victims, and mule accounts across jurisdictions further complicate fraud prevention efforts. Concerns about who would develop, control, and govern the interoperation of fraud registries add to the complexity.

Tracking fraudsters and mule accounts remains ineffective, highlighting the need for a mechanism to place fraudulent transactions on hold for validation or potentially reverse them when necessary. Consistent cross-border recovery of funds after fraud is also challenging, necessitating a standardised approach to returning money to customers. While Confirmation of Payee (CoP) (Pay.UK (2020)) and Verification of Payee (VoP) (EPC (2024)) processes can confirm the payee, they cannot restrict mule accounts and need to be part of comprehensive fraud controls. Prevention at the initiation of a transaction is deemed the most effective point to stop fraud. However, the consistency and trustworthiness of shared data vary due to different levels of maturity among jurisdictions. The establishment of interoperable trust frameworks enabling secure validation is likely to offer a more systematic way to block fraudsters at the onboarding stage.

Jurisdictional challenges, including different privacy laws and interpretations, complicate data sharing and fraud prevention efforts. Limited collaboration among jurisdictions further exacerbates these challenges, making it difficult to implement effective cross-border fraud prevention measures. Additionally, the success of solutions in certain parts of the world is often due to jurisdictional similarities, so achieving similar success across different regions may be more challenging.

2.2. How do standards of fraud prevention differ across jurisdictions?

The domain of cross-border payments is significantly impacted by varying fraud prevention methods, which are influenced by the different maturity levels and practices across jurisdictions. Firstly, there are the industry standards that guide certain practices: Market-level differences complicate the landscape of fraud prevention. There are notable disparities in the effectiveness of fraud prevention measures at the network level compared to the institutional level across different markets. For instance, some markets may have robust network-level controls but weaker institutional-level measures, or vice versa. This inconsistency extends to the level of fraud control between banks and non-bank PSPs.

Differing levels of risk tolerance across jurisdictions and institutions within those jurisdictions also play a significant role in the variation of fraud measures. Different markets have varying levels of tolerance for risk, which influences the stringency of their fraud prevention measures. Markets with a low-risk tolerance may implement more stringent fraud controls, while those with a higher risk tolerance may adopt less rigorous measures. This variation can lead to inconsistencies in the effectiveness of fraud prevention across jurisdictions, making it challenging to achieve a unified approach to combating fraud in cross-border payments.

Digital identity and trust frameworks support the combating of fraud via more sophisticated verification services and could be a powerful fraud solution for interlinked FPS, as well as positively impacting resilience assessment. Trust frameworks are defined as the set of rules and policies that govern

operations and interactions between parties (NIST (2018)). However, the introduction of such frameworks, and the extent to which they are supported by legislation or the maturity of national identity management systems, varies significantly across jurisdictions. Moreover, the activation of such frameworks at a national level, let alone interoperability, requires a strategic and collaborative approach between policymakers, public authorities, banks, fintechs, and central banks. It should be noted that, by virtue of their existing and widespread connectivity domestically, interconnected FPS rails could potentially represent a critical network for the transmission and sharing of bank-verified customer attribute data cross-border for identity and verification in fraud prevention use cases.

Fraud prevention will also be affected by the ongoing development and adoption of next-generation Secure Payment Confirmation (SPC) authentication by the Web Payments Working Group of the W3C.[1] At present, FPS operators may be underrepresented in the development of what may be a crucial standard for global e-commerce payments.[2] The ability to "pause" payments when fraud is suspected is essential for protecting financial institutions and their customers. Currently, there is limited consistency across jurisdictions, with Brazil and the UK being among the few jurisdictions to establish legal provisions for this. However, having a robust legal framework that allows such actions is only part of the solution. The alternative view involves the reputational risks associated with these actions, particularly concerning false positives, where legitimate transactions are mistakenly flagged as suspicious. This highlights the need for a sound legal framework that provides the necessary authority for financial institutions to halt transactions while being consistent across jurisdictions. Differences in the criteria for what constitutes a fraudulent transaction create difficulties in applying these solutions consistently across multiple jurisdictions.

Furthermore, differences in regulatory guidance also result in varying standards. Banks are often subject to stricter regulatory oversight and may implement more rigorous fraud prevention measures compared to non-bank PSPs, which often operate under different regulatory frameworks. The lack of regulatory consistency across jurisdictions was previously highlighted as an issue in a report by the FSB on regulating and supervising bank and non-bank service providers offering cross-border payment services (FSB (2024)). For instance, the report emphasises how inconsistent implementation of, or variations in, the application of AML/CFT measures – including customer due diligence (CDD) requirements – across jurisdictions can slow down processing times and increase the cost of cross-border payments. These differences in regulatory frameworks create challenges in achieving a harmonised approach to fraud prevention and efficient cross-border transactions.

These disparities between jurisdictions significantly impact critical processes such as KYC procedures and the management of mule accounts. In jurisdictions with more advanced fraud prevention frameworks, KYC processes involve thorough verification of customer identities, making it more challenging for fraudsters to infiltrate the system. Conversely, in regions with less stringent KYC requirements, the process may be more superficial, enabling fraudsters to exploit these gaps and open accounts with relative ease.

[1] See W3C: Secure Payment Confirmation

[2] See W3C: Participants Web Payments Working Groups.

3. FRAUD PREVENTION INITIATIVES – SELECTED CASE STUDIES

3.1. Fraud pattern, anomaly and mule account detection

Pay.UK collaborative fraud detection pilot with industry

Fraud often involves many transactions and multiple "hops" between accounts that only become evident when the entire pattern of transactions in a network is viewed together. This, combined with the use of AI, enables the instant disruption of emerging patterns of fraud. In May 2024, Pay.UK announced the completion of a fraud detection pilot in collaboration with the UK payments industry and three fraud prevention solution providers – Visa, Featurespace, and Synectics Solutions. The pilot trialled a new overlay service that allows participating UK PSPs to analyse money flows and use predictive intelligence to proactively detect emerging patterns of fraud and help to safely and securely prevent crime before it occurs (Pay.UK (2024a)).

Results from the pilot overall showed an average 40% improvement in fraud detection at a 5:1 false positive rate. In the case of Visa, the pilot's advanced network approach detected over 54% of scams that had not been identified by individual bank systems. The methodology involved the analysis of billions of historic UK retail payments over a 12-month period, generating a risk score that indicates the likelihood that an account-to-account payment is part of a fraudulent transaction. This contributes an additional layer of information to PSPs to detect fraud at its initiation and take actionable steps to prevent fraudulent activities. The benefits of the solution are believed to include more robust security, seamless integration with existing fraud and risk solutions, scalability to the size of the network, and real-time analysis of transaction data to provide almost instant information on the likelihood of fraudulent transactions.

EBA CLEARING's Fraud Pattern and Anomaly Detection (FPAD)

PSPs have traditionally worked in silos, each investing in separate systems to protect customers against fraud in payments. This fragmented approach leaves many vulnerable to common threats, as they lack a unified view of risk. European PSPs are now starting to collaborate to improve the overall safety of the payments ecosystem. Until recently, no shared pan-European functionality existed to specifically address credit transfer risks. Launched in March 2024, EBA CLEARING's fraud-fighting functionality FPAD provides STEP2 and RT1 participants with access to a wide range of real-time fraud prevention and detection tools. FPAD enables participants in its two core services – STEP2[3] and RT1[4] – to elevate their fraud prevention capabilities. It does so by enriching the PSP's individual risk views with insights that only a network view can provide.

FPAD also helps PSPs comply with regulatory requirements related to fraud prevention, such as those stipulated by the Instant Payments Regulation or the draft Payment Services Regulation (PSR) (EBA Clearing (2024)). These tools support the real-time identification of fraud patterns and anomalies. The database ingests over 30 million new transactions daily, enabling PSPs to assess fraud risks before payments are made and investigate post-transaction threats. PSPs can choose from various detection models within FPAD (including VoP) and customise risk assessments based on their business needs. While FPAD offers valuable insights, it does not make decisions for PSPs, allowing them to act as they see fit. Early adopters have already reported significant reductions in fraud losses, with some experiencing up to a 35% decrease within the first six months.

Reserve Bank of India's MuleHunter.AI

[3] A pan-European Automated Clearing House (ACH) service for processing SEPA Credit Transfers (SCT)—standard euro-denominated payments across the Single Euro Payments Area.

[4] A real-time infrastructure for processing SEPA Instant Credit Transfers (SCT Inst), enabling immediate euro payments 24/7 across SEPA countries.

The Reserve Bank of India (RBI) has been taking various measures in coordination with banks and other stakeholders to prevent and mitigate digital fraud in the financial sector. These include RBI guidelines for strengthening cybersecurity, cyber fraud prevention, and transaction monitoring. Money mule accounts are a common method used by fraudsters to channel the proceeds of fraud.

The RBI ran a hackathon on the theme "Zero Financial Frauds," which included a specific problem statement on mule accounts to encourage the development of innovative solutions to contain their use. Another initiative in this direction is the AI/machine learning-based model called MuleHunter.AI™, being piloted by the Reserve Bank Innovation Hub (RBIH), a subsidiary of the RBI. This model enables the efficient detection of mule bank accounts. A pilot with two large public sector banks has yielded encouraging results. Banks are encouraged to collaborate with RBIH to further develop the MuleHunter.AI™ initiative to address the issue of mule accounts being used for committing financial frauds (Reserve Bank Innovation Hub (2024)).

Project Tazama

Across Africa, stakeholders in FPS have significant opportunities to enhance security measures through the adoption of robust, risk-based KYC processes. A shared KYC facility for FPS could play a crucial role in mitigating identity theft and SIM swap incidents,[5] which are prevalent in several African jurisdictions. Increasing end-user awareness about the risks and methods employed by criminals can further address social engineering fraud.

Providing an expedited redress mechanism, such as an additional recourse avenue for end users, could enhance user trust. Advancements in real-time fraud detection, exemplified by the open-source project Tazama, could offer further security enhancements (AfricaNenda (2024)). Project Tazama is a real-time transaction monitoring software built for fraud and money laundering detection to stop fraud before it happens by implementing simple or complex rules and fraud detection controls to assist in supporting AML activities (Tazama (2024)).

3.2. Centralised databases, information sharing, and taxonomies

Collaboration and information sharing are emerging as key strategies in the fight against fraud, both within the financial sector and across sectoral and geographic boundaries. This aligns with an increased emphasis on transaction monitoring, including real-time fraud screening and manual interventions. Banks and other PSPs are developing industry groups to share intelligence on fraud methods and strategies to combat them. The lack of awareness of best practices in fraud prevention is a notable gap. In Europe, the European Commission is exploring how this can be addressed through the PSR. The PSR aims to provide a regulatory framework that facilitates the sharing of information and the implementation of best practices across the European Union (EU). It should be noted that while the EU is providing a framework for addressing fraud within the region, the types of fraud and associated risks vary between different markets. Despite the benefits of sharing information, it is equally important to understand how this information can be best utilised to prevent fraud.

Robust data protection methods are paramount to ensure the feasibility of identifying patterns and anomalies in transaction data. Identifying these patterns is crucial for all participants in the payment ecosystem to effectively combat fraud. Some governments are actively encouraging this effort, such as Brazil's November 2023 circular mandating financial institutions to share fraud-related data through a secure electronic system, or Malaysia's recently launched National Fraud Portal.

RBI's Digital Payments Intelligence Platform (not yet live)

[5] SIM swap incidents refer to a form of identity theft where a fraudulent actor tricks a network provider into swapping a phone number to a new SIM card which is controlled by the fraudulent actor, meaning they can intercept secure communications sent to the victim and access confidential information and data

The suggestion of a database for utilities has been proposed as a potential solution for enhancing fraud prevention. In line with this, the RBI has proposed the establishment of a Digital Payments Intelligence Platform, which will harness advanced technologies to mitigate payment fraud risks. This platform is envisioned to enable network-level intelligence and real-time data sharing across the digital payment ecosystem (RBI (2024)).

Such a database is believed to provide significant benefits, such as the aggregation and analysis of transaction data from multiple sources,[6] which would facilitate the identification of fraudulent activities. Additionally, this approach could foster better coordination and information sharing among different entities, enhancing the overall effectiveness of fraud prevention measures. However, implementing such a database would necessitate addressing concerns around data privacy and security to ensure compliance with regulations like the General Data Protection Regulation (GDPR) in the EU.

Bank Negara Malaysia and PayNet's National Fraud Portal

The National Fraud Portal (NFP) has been launched by Bank Negara Malaysia (BNM), Payments Network Malaysia Sdn. Bhd. (PayNet), and financial institutions to enhance the operational capabilities of the National Scam Response Centre (NSRC). The NFP automates the process of handling scam reports and tracing stolen funds, enabling swift fund recovery and effective information sharing among financial institutions. It also supports data-driven assessments of mule accounts, streamlining their identification and management (BNM (2024)). The financial industry has adopted standardised procedures for reporting and handling mule accounts, ensuring victims can still access basic financial services. These measures are part of BNM's broader strategy to combat financial scams, which includes ensuring fair treatment of victims and joint accountability in fraud cases.

Since its launch in April 2024, the NFP has reduced the time required to trace stolen funds by 75% and increased the amount of frozen illicit funds by 28% (Fintech Malaysia (2024)). The NFP has also improved the detection of mule accounts by 14% and expanded its reach to include major e-wallet providers such as TNG eWallet. In 2023, BNM and financial institutions blocked 383 million MYR worth of unauthorised transactions, while phishing and malware fraud cases showed a downward trend. Victims are encouraged to contact the NSRC hotline for swift action.

Euro Banking Association's fraud taxonomy

The Euro Banking Association's (EBA's) fraud taxonomy serves as example an for classifying specific fraud cases collaboratively. This taxonomy provides a structured framework for identifying and categorising various types of fraud, which is critical for effective fraud prevention and mitigation (EBA (2024)). The taxonomy breaks down complex fraud scenarios into detailed categories, enabling the collection of more granular fraud data. By implementing a consistent vocabulary and terminology, it facilitates alignment between payment service providers (PSPs) for internal reporting and supports the sharing of fraud intelligence and data across institutions. This approach is designed to help detect and prevent fraud across borders effectively. This includes:

- Method: How was the victim contacted?
- Modus: What method was used to commit the fraud?
- Initiator: Who initiated the fraudulent transaction (ie the victim or the fraudster)?
- Labels/tags: What additional details can be added regarding the fraudulent event?
- Payment instruction: Was this an account-to-account (A2A) transaction or a card payment?

[6] In India, a set of digital identity products have been built around Aadhaar, India's national identity program implemented in 2009. Roughly 95% of the Indian population has an Aadhaar number. The number is used with a variety of digital identity products that enable E-KYC authentication, access to digitally signed and universally accepted copies of lifetime records, and the digital signing of official documents.

This information enables experts to develop more detailed and accurate data on the methodologies used across jurisdictions, allowing for a more effective response to fraud incidents. The taxonomy is intended to be used by PSPs in several key ways. It facilitates easier and faster data-point collection, accelerates transaction tracking, and supports advanced model training. Additionally, it enhances fraud analytics, prevention, and detection by employing a standardised categorisation of fraud types and a common vocabulary for fraud. This approach enables firms to effectively identify, share, and compare fraud trends and data. Further benefits include improved internal and external fraud reporting, which is aligned with the Payment Services Directive 2 (PSD2) Fraud Reporting Guidelines. It also optimises fraud response processes, such as customer support, investigations, and case handling, while promoting more effective customer and employee education on fraud prevention and mitigation.

Australian Financial Crimes Exchange

The Australian Financial Crimes Exchange (AFCX) is an independent, not-for-profit organisation that serves as the primary channel for coordinating efforts to combat financial and cybercrime in Australia. The AFCX Exchange functions as a collaborative platform where members can securely share and access information and intelligence related to financial and cybercrime (AFCX (2024)).

One of its key tools, the Fraudulent Reporting Exchange (FRX), is a secure network that allows financial institutions to efficiently report and address fraudulent activities. Additionally, AFCX IQ is a comprehensive data pool for checking and screening previous fraudulent activities or identity compromises. The AFCX membership includes major financial institutions, payments platforms (such as Australian Payments Plus, operators of the NPP FPS), and the Australian Taxation Office.

3.3. Pre-validation and payment messaging data

Swift payment pre-validation

Swift's payment pre-validation service consists of a set of application programming interfaces which can be called before sending a payment instruction. These services enable debtor agents to validate specific fields within a payment instruction (Swift (2024)). The primary objective of the Swift pre-validation APIs is to reduce the number of payment rejections caused by incorrect account details, identifiers, and codes, as more than 5% of payment transactions currently fail to achieve straight-through processing (STP). Beyond this, the technology also provides an effective mechanism to ensure that the recipient of the funds is the correct beneficiary. By calling a set of API services before sending a payment instruction, debtor agents can validate fields such as whether the account is able to receive funds, whether the account name matches the provided details, and the expected payment purpose, among other validation categories.

Currently, 297 banking groups are subscribed to the solution, with over 50 banks implementing it and 81 banks having the solution live. Swift aims to further enhance the service by increasing the number of validators and improving the quality of validation results. This initiative could serve as a robust cross-border payment solution that addresses fraud at its source. Pre-validation is highlighted as a critical consideration in this context. However, as with other solutions like VoP and CoP, the full potential of these practices has yet to be fully explored. Progress in this area is often hindered by concerns surrounding data protection laws, which require careful handling of personal data. Addressing these regulatory concerns and advancing the exploration of pre-validation could significantly strengthen fraud prevention efforts.

Confirmation of payee and verification of payee

One approach to addressing APP fraud is to ensure that the majority of fast payments are made in response to requests originating from channels that fully validate the legitimacy of the beneficiary. Where necessary, these channels should guarantee the beneficiary's bona fides. Such channels could include wallets, e-commerce services, recurring payments, or business-to-business (B2B) and person-to-person (P2P) "overlay" services (eg those based on open banking or request-to-pay services). In these cases, the beneficiary would be subject to scheme rules and KYC checks by a PSP, regardless of national borders.

By utilising these mechanisms, the number of "ad-hoc" payments to unknown or potentially fraudulent beneficiaries can be minimised. However, achieving this requires a mature overlay ecosystem, particularly in cross-border contexts. In regions where such overlays do not exist, remaining P2P transfers should be subject to enhanced transaction-level checks. Solutions like CoP and VoP are examples of limited measures designed to help payers and their PSPs address this gap. Similar arrangements could potentially be implemented across borders, with VoP as a SEPA-wide solution serving as a possible model.

The increased awareness of VoP and CoP in the EU and in the UK marks a significant step towards enhancing payment security. However, concerns have been raised about the feasibility of extending these solutions to a cross-border context. Currently, VoP and CoP remain primarily regional solutions, and there is a consensus that substantial work is needed to adapt and implement these mechanisms on a global scale. Fraudsters tend to exploit weaker points in the system. For instance, in the UK, before CoP was universally implemented, fraudsters shifted their activities to institutions where the solution was not available. By further developing and refining these solutions, their effectiveness could be significantly enhanced in a cross-border environment, providing stronger safeguards against APP fraud.

BIS Innovation Hub Project Mandala

Project Mandala is a proof-of-concept run by the BIS Innovation Hub (BISIH) Singapore Centre in collaboration with the Reserve Bank of Australia, the Bank of Korea, the BNM, and the Monetary Authority of Singapore, alongside financial institutions. The project aims to ease the policy and regulatory compliance burden by automating compliance procedures, enabling real-time transaction monitoring, and increasing transparency and visibility around country-specific policies (BIS Innovation Hub (2024)).

The project has demonstrated that regulatory compliance can be seamlessly integrated into cross-border transaction protocols. A compliance-by-design decentralised system has been developed to enhance the efficiency of cross-border payments by embedding regulatory compliance within a network of financial institutions and central banks. This innovative decentralised architecture is built on three core components:

- Peer-to-peer messaging system: This component facilitates secure and direct communication between financial institutions, ensuring that transaction data is transmitted efficiently and securely.
- Rules engine: The rules engine evaluates transactions against a comprehensive set of regulatory requirements and compliance rules, ensuring that all necessary checks are performed.
- Proof engine: Once all checks are completed, the proof engine generates a verifiable compliance proof, certifying that the transaction adheres to regulatory standards.

This architecture ensures that all compliance checks are completed before a payment is initiated, significantly reducing the risk of non-compliance and enhancing the security of cross-border transactions. Once the checks are successfully completed, a compliance proof is generated, which can accompany any digital settlement asset or payment instruction. Importantly, to preserve privacy, the compliance proof can be verified without revealing underlying customer data, using advanced cryptographic techniques to maintain data integrity and confidentiality. Additionally, this decentralised approach reduces reliance on central intermediaries, thereby lowering transaction costs and increasing the speed of cross-border payments. By embedding regulatory compliance directly into the transaction process, the system not only improves operational efficiency but also fosters trust among participating financial institutions and regulatory bodies.

Pay.UK Enhanced Fraud Data

Pay.UK collaborated with the wider payments industry to develop the Enhanced Fraud Data (EFD) messaging standard, designed to carry data in a pre-agreed, structured format (Pay.UK (2024b)). The standard was built to support interoperability across relevant domestic and international schemes and initiatives, including CHAPS, CBPR+, SEPA, CGI-MP, and UK Open Banking. It also aligns with key standards

for digital ID, such as the internationally recognised OpenID Connect for Identity Assurance (OIDC IDA) and the UK's Digital ID and Trust Framework (DIATF), as well as ISO 20022 naming conventions. Additionally, the design incorporates extensibility, allowing it to support multiple applications.

The enriched data-sharing capabilities between banks and other PSPs have enabled the wider development of a peer-to-peer fraud prevention API solution. This solution can operate in a similar way to CoP, leveraging the same directory service. EFD enables fraud analysts to make enhanced risk-based decisions on transactions by providing a comprehensive set of data attributes to both the sending and receiving organisations before the payment is initiated. The solution is expected to improve fraud detection rates while reducing false positives, ultimately leading to fewer fraudulent transactions and financial losses. EFD is one of three measures introduced by the UK's Payment Systems Regulator (PSR) to combat APP scams. Specifically, one of the measures tasks the industry with enhancing intelligence sharing, and the EFD solution facilitates this by enabling enriched data fields to be shared between PSPs. This can be implemented as a standalone measure or in conjunction with existing fraud monitoring tools.

3.4. Transaction limits and delays

Pix Brazil Transaction Limits

Transaction limits are an effective method for preventing fraud, with two primary approaches to implementing these limits. The first involves placing restrictions on the number of transactions that can be made within a specific period, while the second sets limits on the value of each transaction being sent (World Bank (2023)). This approach has been adopted in jurisdictions such as Brazil, where the FPS Pix allows users to establish maximum transaction limits per payer, per day, and per month (BCB (2024)). By enabling payers to define their own limits, this system provides greater autonomy for users to align transaction activity with their risk appetite, thereby enhancing protection against certain types of fraudulent transactions.

UK Suspicious Payment Delay

Some jurisdictions are exploring legislative measures to mandate the blocking or delaying of payments to investigate suspected fraudulent activities. In the UK, the Payment Systems Regulator (PSR) is introducing new rules that allow payment service providers to delay payments for up to 72 hours if there are reasonable grounds to suspect fraud. This delay provides additional time for investigations, potentially preventing fraudulent transactions from being completed (HM Treasury (2024)).

3.5. Digital identity

eIDAS

eIDAS is a regulation established by the European Union to promote the use of digital IDs across member states, aiming to build confidence in electronic interactions and foster seamless digital services within the EU (European Commission (2024)). eIDAS has evolved over time. eIDAS 1.0 established a framework for digital IDs to facilitate cross-border transactions.

The updated regulation eIDAS 2.0 focuses on the interoperability of digital IDs (cross-border e-IDs) across the EU. While its implementation is ongoing, it includes provisions for a secure digital ID wallet, enabling users to authenticate payments and access various services within the EU. eIDAS 2.0 aims to enhance digital payments by allowing users to perform secure transactions using their verified identity, thereby reducing fraud risks. It also simplifies authentication by enabling users to rely on a single digital ID across multiple platforms, streamlining the checkout process. Furthermore, eIDAS supports compliance with EU regulations on ID verification, ensuring that payment services meet robust security standards.

4. KEY CONSIDERATIONS AND ACTIONS FOR INDUSTRY

4.1. Payment networks and FPS operators seek to establish interoperable fraud registries

To effectively combat fraud in cross-border payments, establishing interoperability among fraud registries linked to different FPS is essential. Such interoperability would facilitate the sharing of information, enable better identification of known fraud perpetrators, and enhance the ability to prevent fraudulent activities. While the exact methodology for sharing this information is yet to be determined, it is critical to develop clear governance frameworks to guide data sharing. These frameworks should define pathways for controlled and secure data exchange under appropriate circumstances. This would ensure that intelligence about fraudsters, victims, and mule accounts can be effectively shared across jurisdictions, strengthening the global effort to combat payment fraud.

4.2. Payment networks and FPS operators seek to leverage technology for enhanced data sharing

To effectively combat fraud in cross-border payments, it is crucial to develop mechanisms that ensure compliance with FATF Recommendation 16 on payments transparency to enhance data visibility across payment networks. While achieving complete transparency may currently be constrained by privacy and confidentiality requirements, alternatives such as tokenisation and other PETs offer promising capabilities to support secure data sharing. However, these interim solutions should not deter the industry from striving toward mechanisms that enable full transparency as a long-term objective. Addressing the fragmented nature of existing data systems is equally important for comprehensive fraud detection and analysis. Leveraging advanced technologies can facilitate the development of effective data-sharing mechanisms, including the use of anonymised data points such as transaction risk indicators or account identifiers.

4.3. FPS operators and payment networks implement robust pre-validation processes

The implementation of pre-validation within payment systems is widely recognised as a valuable step in securing transactions at the initial stages. Current systems are often not equipped to accommodate these processes effectively, leaving transactions vulnerable to fraud. A shared data model and common set of standards would provide a consistent, interoperable framework for verifying payee details across borders. This alignment reduces fragmentation, eliminates gaps that fraudsters can exploit, and enables real-time, accurate validation regardless of jurisdiction. Standardisation also simplifies integration, reduces duplication of effort, and ensures a unified approach.

By setting up systems that support pre-validation and testing of payment routes, the industry can significantly reduce the risk of fraudulent activities. PIE Task Team 2 has observed effective solutions, such as Swift's pre-validation APIs, CoP, and VoP, all of which aim to implement an effective form of pre-validation. If implemented pre-validation is implemented consistently across jurisdictions, there is an opportunity to ensure that transactions are thoroughly vetted before execution, thereby enhancing the security and integrity of cross-border payments. These pre-validation processes should be designed to balance the need for security with the user experience, ensuring that disproportionate transaction delays are sufficiently mitigated. However, it should be noted that while pre-validation is an effective tool, it only addresses a limited subsection of fraud. This is because if a payer is convinced that the payee is not a bad actor, pre-validation will not detect an issue with the transaction.

4.4. PSPs should work collaboratively to share KYC best practices with peers globally and adopt leading KYC practices

Establishing stringent and comprehensive KYC processes across all jurisdictions is crucial for preventing fraudsters from opening accounts and exploiting system vulnerabilities. The varying levels of KYC across different regions create inconsistencies that fraudsters can exploit. By sharing KYC best practices globally, the industry can promote a consistent, high standard of fraudster and mule account detection. This approach would involve understanding what effective practices look like, providing the ability for PSPs to identify and adopt the most effective practices from other jurisdictions, and ensuring that all markets, regardless of their current level of maturity, have access to and understand what best practice entails.

It may also be beneficial to focus on the parties that can support the sharing of leading practices, such as the Wolfsberg Group or ISO 37003, and to establish practical mechanisms for sharing effective practices. Furthermore, suggesting mechanisms for continuous improvement and adaptation of KYC practices in response to evolving fraud tactics will be vital. This could include regular assessments of fraud tactics, feedback loops from industry stakeholders, and the establishment of forums for sharing insights and experiences. Additionally, a key area of focus should be KYCC, given the increasingly multi-layered nature of payment value chains. Understanding the customers of a firm's customers can provide deeper insights into potential risks and enhance overall fraud prevention efforts.

This key consideration does not suggest a minimum standard that all PSPs should follow due to the potential operational implications but highlights the opportunity to increase global awareness of the most optimal procedures and encourages a set of standards to be adhered to for mutual benefits. International standards-setting bodies are in an optimal position to address the requirement for mutually agreed standards across jurisdictions. This is important to ensure that KYC processes have mutual recognition and that all countries "automatically" recognise the verification without adding additional requirements at a national level.

4.5. Industry participants leverage advanced technologies for fraud detection, shaped by their role in the ecosystem

The integration of advanced technologies, particularly AI, PET, and federated learning, into the fraud detection value chain is essential for identifying anomalies and enhancing fraud prevention capabilities. At an individual firm level, advanced technologies like graph analytics can significantly enhance fraud detection in cross-border payments by providing a more comprehensive view of complex relationships and patterns. The current low use of AI in the payment industry represents a significant gap that needs to be addressed through PSPs actively exploring potential applications. Applications of AI will be shaped by the role each PSP plays within a transaction. For example, in push payment scenarios, the payer's PSPs will tend to focus on the protection of fraud victims, while the payee's PSPs would typically prioritise mule detection, including graph analysis and behavioural approaches. Payment system operators may focus on use cases around data sharing.

Advanced technologies can analyse vast amounts of historical transaction data to refine and enhance the effectiveness of transaction risk indicators (TRIs), which are a key recommendation of the Wolfsberg Group. AI can also analyse vast amounts of transaction data in real time, identifying patterns and anomalies that may indicate fraudulent activities. Additionally, developing TRIs, establishing thresholds, and implementing structured payment methods would aid in recognising and addressing fraudulent transactions. This has proven effective in Pay.UK's collaborative machine learning-driven fraud detection pilot with industry. By leveraging advanced technologies, the industry can significantly improve its ability to detect and prevent fraud in cross-border payments. However, human oversight and review of AI-driven solutions remain important to ensure effective and accurate decision-making.

4.6. Industry associations and international standards setters foster industry collaboration and regulatory alignment

Effective fraud prevention in cross-border payments requires robust industry collaboration and alignment with regulatory frameworks. To foster collaboration among industry stakeholders, specific strategies should be implemented, including regular forums, workshops, and joint initiatives that facilitate the sharing of best practices and address common challenges. Industry associations can play a key role in facilitating anonymised case studies and incident retrospectives, allowing members to learn from one another without reputational risk.

Collaboration can also go deeper than knowledge sharing. The establishment of interoperable trust frameworks, enabling secure validation, is likely to offer a more systematic way to block onboarding fraudsters at source. PIE Task Team 2 considers the role of international standard-setting bodies as important in this context, as they are positioned to provide central support for standardising data models and APIs, which are a crucial step towards more effective knowledge sharing.

Regulatory-driven initiatives play a significant role in shaping industry practices, and establishing a consistent legal framework for data sharing and the interoperability of trust frameworks would facilitate global collaboration and enhance the effectiveness of fraud prevention measures. This is particularly important given the potential resistance from organisations regarding their willingness to participate in data-sharing activities. By fostering industry collaboration and aligning with regulatory requirements, the industry can promote a more cohesive and secure payment ecosystem.

5. KEY CONSIDERATIONS AND ACTIONS FOR PUBLIC SECTOR

The implementation of effective fraud prevention measures in cross-border payments necessitates robust public sector support, particularly to provide clear definitions and regulations. These recommendations by PIE Task Team 2 are outlined in this section.

5.1. International standard setting bodies and operators of cross-border payment systems[7] act as a catalyst for the adoption of universally accepted definitions for fraud

Currently, the responsibility of identifying potentially fraudulent payments is generally placed on the private sector, which operates at its own risk. Additionally, the lack of standardised definitions across jurisdictions creates inconsistencies and vulnerabilities. Although on the surface the definitions may seem complete, across different jurisdictions there are gaps that allow misinterpretation and create opportunities for fraudsters to exploit. There is a requirement to provide clarity on the detailed definitions of components of the instant payment journey.

Therefore, there is a significant opportunity for the public and private sectors to collaborate in establishing universally accepted definitions that institutions can rely on. Such collaboration would provide a foundation for standard practices that can be implemented globally, thereby enhancing the overall security of cross-border payment systems. However, establishing a mechanism to regularly update definitions as fraud tactics evolve is paramount.

[7] Operators of cross-border payments systems can be defined as an entity that manages and operates a payment system where transactions involve funds transferred between countries.

5.2. Regulators globally consider implementing regulations to allow PSPs to effectively intervene in fraudulent activities

Adopting approaches similar to those in the United Kingdom, where transactions can be paused upon suspicion of fraud, in Brazil, where Pix has implemented transaction limits, or in Singapore, where a 12-hour cooling-off period is imposed upon activation of a digital security token during which 'high-risk' activities cannot be performed, should be considered. The impact of these initiatives could be maximised if led by local regulators, as they could co-ordinate the industry towards a more favourable outcome. While the idea of escrow or similar mechanisms may negate the benefits of instant payments, and customers may become frustrated with delays for legitimate transactions, it highlights the fact that these competing outcomes need to be reviewed, and solutions tabled to address the various use cases.

Regulators could also play a crucial role in protecting customers from harm in cross-border payment scenarios where there is a high likelihood that they have been victims of fraud. This could be wide-ranging and include defining reasonable time periods and justifications to ensure that interventions do not unduly inconvenience customers, creating redress mechanisms, as well as clear processes for customers to raise complaints or manage disputes. As explored previously, the need for a sound legal framework that provides the necessary authority for financial institutions to halt transactions and is consistent across jurisdictions would be the most effective solution. However, differences in the criteria for what constitutes suspicious transactions create difficulties in applying these solutions consistently across multiple jurisdictions. Therefore, these definitions should be developed with a domestic focus first, with a view to harmonise cross-border. Regulators and international standards-setting bodies should work together to harmonise these definitions so that these mechanisms can be implemented effectively with key corridors, wherever possible.

5.3. Legislators bring all parties into a regulatory framework to ensure the right actions are taken

It is crucial to consider where fraud typically originates, including the role of players outside the financial services sector, such as telcos (which can be impacted by SIM farms[8], account takeover via telephony, and scam call centres) and large social media platforms (which may host fraudulent communications and advertisements).[9] All relevant parties need to be brought into a framework that incentivises and engages them to take steps to disrupt those who seek to abuse their infrastructure. Efforts to reduce fraud at source could also include more widespread use of bank-authenticated onboarding, particularly for merchant sites.[10] Lessons learned from information and best practice sharing when dealing with cybersecurity threats and transaction-related fraud threats suggest that a multi-institutional approach is most effective.[11] Public authorities are best positioned to arbitrate these efforts, encouraging firms to share instances where effective solutions or practices have been implemented.

[8] SIM farms refer to an environment where multiple SIM cards are managed simultaneously, with common uses involving spamming, fraud and avoiding messaging restrictions

[9] Fraud origination in this instance is defined as when the fraudster initially makes contact with the victim, not the platform or mechanism in which the fraudulent activity is completed.

[10] This emerging trend is evidenced by parallel developments and product strategies in the EU (EPI), France (Bconnect.net), Spain (Bizum), India (Aadhar / UPI), Australia (AP+ ConnectID), Canada (Interac), Singapore (MAS) and the Nordics (BankAxept BankID)

[11] See also the Scams Prevention Framework Bill 2025 recently passed by the Australian Parliament, which addresses the financial sector, telcos, and social media platforms in a whole of ecosystem approach to reducing losses through scams including APP frauds.

5.4. Regulators should consider enforcing the need for legislation to support the establishment of central fraud repositories/exchanges

Countries with advanced FPS have successfully established central repositories or exchanges for fraud data through their authorities. AML frameworks typically contain a "tipping-off" provision that restricts the sharing of information indicating that a suspicious transaction or matter report has been or will be made. It is important that such frameworks be adjusted (where necessary) to allow for the sharing of information with fraud repositories or exchanges, including those operated by the private sector. The implementation of such systems should be viewed as a first step in the journey towards effective real-time information sharing.

Understanding how countries have achieved central fraud repositories/exchanges can provide valuable insights for other jurisdictions. An example of this is the National Fraud Portal in Malaysia. The RBI, over the years, has undertaken a number of measures to enhance the safety and security of digital payments and maintain public confidence in digital payment systems. Many frauds occur by influencing unsuspecting victims to make payments or share credentials. While the payments ecosystem takes various measures on an ongoing basis to protect customers from such frauds, there is a need for network-level intelligence and real-time data sharing across payment systems. However, the implementation of such arrangements must initially focus on establishing information-sharing mechanisms before considering real-time sharing. Further, the coordinated support of the public sector across jurisdictions is essential to ensure that data privacy legislation allows the industry to share information for the purpose of combating fraud.

5.5. Legislators enable the private sector to deliver effective fraud mitigating solutions

The public sector should be open to new models proposed by the private sector, focusing on desired outcomes while allowing the private sector to develop solutions. Enabling frameworks that set the right structures may be necessary for the private sector to deliver effective solutions. For example, in the EU, the recent AI Act expressly acknowledges that the use of AI for the purpose of detecting fraud in the offering of financial services is not considered "high risk" within the meaning of the legislation. Consolidating regulatory efforts to drive outcomes and establishing regulatory sandboxes across jurisdictions can help achieve consistency in fraud prevention measures. However, the potential risk that actions of individual firms pose to the system should be considered to ensure that the approach is proportionate to this risk and that there is sufficient accountability across the different market players.

5.6. Central authorities encourage the implementation of digital identity

Digital identity provides sophisticated verification services that support the combating of fraud and could serve as a powerful solution for interlinked FPS, as well as cross-border payments more generally. By leveraging this new form of identity, financial institutions can ensure more accurate and reliable identity verification processes. However, it should be acknowledged that, if implemented incorrectly (eg KYC chain reliance, inadequate controls, or poor adoption rates), it may provide an entry point for fraudsters to exploit. Through the implementation of digital identity solutions, advanced tools and technologies for verifying the authenticity of an individual's identity can reduce the likelihood of identity theft and impersonation. This makes it more difficult for fraudsters to create fake identities or use stolen credentials to set up mule accounts or circumvent blacklists, thereby increasing protection for customers. It could also enable PSPs to authenticate themselves and their communications to their clients, reducing bank impersonation fraud, although this is often done within their own apps.

5.7. Authorities and private sector entities invest in consumer education and improve financial literacy

Despite the preventative measures that financial institutions can implement, the issue remains that consumer behaviour drives fraud outcomes. Social media platforms present an opportunity to provide widespread financial education to help individuals increase their awareness of fraud tactics, understand secure financial practices, and improve their decision-making skills. However, it is important to acknowledge that delivering this level of customer education to vulnerable populations may be challenging, and campaigns must have sufficient reach to address these groups.

In addition, ensuring adequate levels of financial education on other platforms where fraud is prevalent – such as marketplaces, telephony, postal, and email channels – is crucial to engage a wide range of market players in educating customers. Previous efforts, such as the eIDAS regulations, have demonstrated success where public/private collaboration and financial education campaigns have effectively raised awareness among end consumers about making and receiving payments. By increasing financial education and awareness at the source of fraudulent activity, individuals are more likely to identify red flags and make informed decisions regarding their finances. They can critically evaluate financial products, services, and offers, reducing the likelihood of falling for fraudulent schemes that promise unrealistic returns or benefits.

5.8. Strengthen transnational law enforcement and inter-agency collaboration

Transnational law enforcement and inter-agency partners should prioritise the development of real-time intelligence-sharing frameworks, coordinated investigations, and joint operational hubs that bring together financial institutions, telecoms, fintechs and cybercrime units. Building on successful models such as Singapore's Anti-Scam Command and West Africa's ECOWAS cybercrime task force, these partnerships should enable rapid disruption of mule networks, scam operations, and laundering corridors – particularly in high-risk regions. Embedding law enforcement within cross-sectoral operations, supported by shared analytics and early warning systems, can significantly increase disruption capacity while reducing harm to consumers and financial systems.

Additionally, agencies should work toward legal and supervisory alignment across borders, focusing on harmonised definitions of digital fraud, streamlined data-sharing protocols, and mutual recognition of enforcement tools. Drawing from ASEAN's Digital Integration Framework and Ghana's Cybersecurity Act, inter-agency collaboration should also include capacity building in jurisdictions that are often exploited as transit points for fraud proceeds. Investing in cyber-forensics, AML supervision, and fraud detection infrastructure in these corridors will close gaps that organised crime networks rely on and enable a globally coordinated, intelligence-led approach to safeguarding cross-border payments.

6. CONCLUSIONS

In conclusion, the domain of cross-border payments faces significant challenges in fraud detection and prevention, requiring a comprehensive and multifaceted approach to address these issues effectively. The fragmented nature of transaction data and the underdeveloped state of pre-transaction checks are key factors contributing to instances of fraud in cross-border payments. To overcome these challenges, it is essential to adopt solutions such as enhancing data visibility and sharing mechanisms, implementing robust pre-validation processes, standardising KYC practices, and establishing a global trust framework. Such a framework could facilitate the secure return of funds or the sharing of compliance check outcomes on a global scale. Additionally, leveraging advanced technologies, such as AI, for fraud detection could provide proactive measures to identify and prevent fraud at its source.

Industry collaboration and regulatory alignment are critical to creating a cohesive and secure payment ecosystem. Public sector support plays an indispensable role in implementing effective fraud prevention measures for cross-border payments. By providing clear definitions, fostering collaboration, harmonising regulations, and supporting innovative solutions, the public sector can significantly enhance the security and efficiency of global payment systems. By fostering a collaborative approach among industry stakeholders, regulators, and public authorities, and by leveraging advanced technologies and standardised practices, the payment industry can substantially strengthen its ability to detect and prevent fraud in cross-border transactions.

REFERENCES

AfricaNenda (2024): *The State of Inclusive Instant Payment Systems in Africa*, November.

Australian Financial Crime Exchange (AFCX) (2024): *Fraud Reporting Exchange*, March.

Bank Negara Malaysia (2024): *National Fraud Portal (NFP) to solidify coordinated efforts in curbing financial scams*, August.

BIS Innovation Hub (2024): *Project Mandala: shaping the future of cross-border payments*, October.

Banco Central Do Brazil (2024): *Combating Money Laundering and the Financing of Terrorism – AML/CFT*, December.

Euro Banking Association (2024): *What is the EBA Fraud Taxonomy?*, December.

EBA Clearing (2024): *FPAD: Fraud Pattern and Anomaly Detection*, December.

European Commission (2024): *eIDAS Regulation*, April.

European Payments Council (2024): *Verification of Payee*, December.

Financial Stability Board (FSB) (2024): *Recommendations for Regulating and Supervising Bank and Non-bank Payment Service Providers Offering Cross-border Payment Services: Final Report*, December.

Fintech Malaysia (2024): *BNM's National Fraud Portal Can Now Trace Stolen Funds in 30 Minutes*, October.

HM Treasury (2024): *New powers for banks to combat fraudsters*, Press release, October.

India National Government Services Portal (2024): *National Cyber Crime Reporting Portal*, December.

NIST (2018): *Developing Trust Frameworks to Support Identity Federations*, U.S. Department of Commerce, January.

Pay.UK (2020): *Overlay Services – Confirmation of Payee*, December.

——— (2024a): *Pay.UK's Fraud Detection Pilot Exceeds Expectations, Detecting Over £112m Worth of Fraud*, May.

——— (2024b): *Enhanced Fraud Data*, December.

Reserve Bank Innovation Hub (2024): *Detect and flag mule accounts in near real-time*, December.

Tazama (2024): *Our Projects – Tazama Transaction Monitoring System*, December.

World Bank (2023): *Fraud Risks in Fast Payments*, October.

Annex: Authors and contributors

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

Organisation	Name
Iberpay	*José Luis Langa (co-Lead)*
UK Finance, JP Morgan	*Katja Lehr (co-Lead)*
AfricaNenda	*Sabine Mensah*
NPCI	*Vinod John*
NPCI	*Rina Penkar*
NPCI	*Amit Bajpai*
Pay.UK	*Daniel Jonas*
Societe Generale Group	*Frantz Teissedre*
Swift	*Mike Truter*
VISA	*Nick Senechal*
UK Finance	*Sairoze Hemani*
EY (UK Finance member)	**Alex Thomas, Thomas Bull**
Additional expert input	**Alla Gancz**