Australian Payments Network

SAFETY BY DESIGN IN PAYMENT SYSTEMS

July 2025

Contents

Executive Summary

Over the past decade, both the marked shift towards digital and the increasing adoption of real-time payment methods – notwithstanding their benefits – have also contributed to a significant rise in economic crime. Payment card fraud in Australia reached A$868 million in the 12 months to June 2024.[1] Reported scam losses totalled A$2.03 billion in 2024, representing a 34.5 percent decrease from the 2022 peak of A$3.1 billion.[2] Globally, an estimated 2-5 percent of GDP (up to US$2 trillion) is laundered annually.[3] These crimes impose costs beyond direct victims, affecting financial institutions through compliance requirements that totalled approximately US$200 billion worldwide in 2023.[4]

This paper reviews the impact of scams on a number of markets but principally Australia and the United Kingdom. It also catalogues some of the effective measures implemented in those markets to mitigate fraud and scams, recognising that no one measure completely mitigates risk, but rather a plethora of responses is required, preferably encompassing a whole of ecosystem approach.

The paper also explores how safety could and should be included by both Payment System Operators (PSOs) and Payment Service Providers (PSPs) in their design phases, particularly in developing fast payment systems (FPS) and pursuing the path to global connectivity. Fundamentally, the paper advocates 'Safety by Design' (SbD) Principles to address scams and fraud. Importantly, a fit for purpose framework of principles, developed by the eSafety Commissioner in Australia, provides PSOs and PSPs with the requisite guidance to achieve the goal of SbD. Through a series of steps, this unique framework articulates service provider responsibilities, user empowerment and autonomy, as well as transparency and accountability.

This paper suggests that the eSafety Commissioner's SbD Principles, which position safety as a fundamental design consideration and were developed through in-depth consultations with large technology and start-up companies, provide a robust foundation for the technology ecosystem. This is substantiated by the extensive array of measures implemented to combat scams and fraud, when viewed through the prism of the SbD Principles. It is contended that SbD should be a cornerstone of the payments ecosystem development process and that inter-governmental, national and international authorities, regulators and private sector bodies should actively support, advocate and, where appropriate, mandate its inclusion in the payments ecosystem in the jurisdictions for which they are responsible.

[1] AusPayNet (2024), 'Fraud Statistics Jul 23 – Jun 24'. Available at <https://www.auspaynet.com.au/resources/fraud-statistics/July-2023-June-2024>.

[2] ACCC (2025), 'Targeting scams: Report of the National Anti-Scam Centre on scams data and activity 2024', March. Available at < https://www.nasc.gov.au/system/files/targeting-scams-report-2024.pdf >.

[3] UNODC (United Nations Office on Drugs and Crime), 'Money Laundering'. Available at <https://www.unodc.org/unodc/en/money-laundering/overview.html>.

[4] Banking Frontiers (2024), 'High cost of financial crime compliance affects quality CX'. Available at <https://bankingfrontiers.com/high-cost-of-financial-crime-compliance-affects-quality-cx/>.

Background

The digital economy has revolutionised how people communicate, conduct business, access services and make payments, bringing significant efficiencies to the transaction process. But while gains in speed and convenience have been achieved, criminals have evolved their methods of exploiting targets, particularly how they perpetrate scams, cyber-crime and money laundering activities, and this has resulted in an erosion of trust. The risk of criminal exploitation and the impact on victims was not fully appreciated *ex ante*. In the past three years, all digital economy sectors implemented aspects of SbD after *ex post* to rebuild consumer trust.

Scams are a shared global problem, for example, scam losses in selected countries are estimated to total:

- UK: £1.17 billion[5]
- Singapore: SG$1.1 billion[6]
- USA: US$16.6 billion[7]
- Australia: A$2.74 billion.[8]

The Global Anti-Scam Alliance (GASA) estimates that in 2024, over US$1 Trillion was siphoned globally by scammers.[9] Putting that in perspective, this figure is larger than the GDP of Switzerland.[10]

In Australia's National Anti-Scam Centre's March 2025 *Targeting scams*[11] report, the most reported payment method for scam losses was bank transfer, which accounted for 44.5 per cent of overall scam losses by value. Bank transfers include transactions via legacy payment rails, such as direct entry (Australia's Bulk Electronic Clearing System, BECS), as well as the domestic FPS, the New Payments Platform (NPP).

Scams in the payments ecosystem impact not just those directly targeted but also affect consumer confidence in the digital economy and the relationship of consumers with their providers of payment services. Therein lies the real challenge for PSPs and PSOs, to inherently incorporate safety in design.

This paper explores the concept of SbD and how it can help address some of the challenges that fraud and scams have caused the payments ecosystem.

[5] UK Finance (2025), 'Annual Fraud Report 2025', May. Available at <https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2025>.

[6] Singapore Police Force (2025), 'Annual Scams and Cybercrime Brief'. Available at <https://www.scamshield.gov.sg/files/Scams%20and%20Cybercrime%20Briefs/2024_annual_scams_and_cybercrime_brief.pdf>

[7] FBI (Federal Bureau of Investigation) (2025), '2024 Internet Crime Report', 23 April. Available at <https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf>.

[8] ACCC (2024), 'Scam losses decline, but more work to do as Australians lose $2.7 billion', Media Release, 28 April. Available at <https://www.accc.gov.au/media-release/scam-losses-decline-but-more-work-to-do-as-australians-lose-27-billion>.

[9] Rogers S (2024), 'International Scammers Steal Over $1 Trillion in 12 Months in Global State of Scams Report 2024', Global Anti-Scam Alliance, 7 November. Available at <https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai>.

[10] World Bank Group, 'GDP (current US$) – Switzerland'. Available at <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=CH>.

[11] See ACCC (2025)

Setting the scene

The scams and fraud cycle follows the same path as the money-laundering cycle. As a single process, it has three distinct stages[12]:

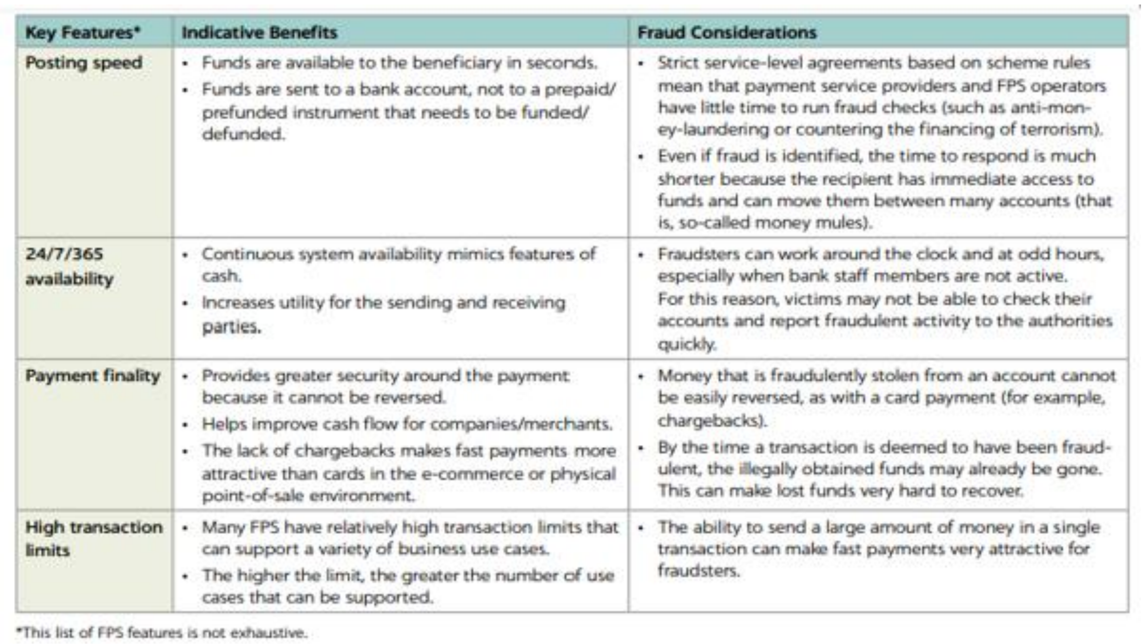
1. Placement – moving the funds from direct association with the crime
2. Layering – disguising the trail to foil pursuit
3. Integration – making the money available to the criminal from what appear to be legitimate sources.

The vast majority of scams[13] in the UK (95.6 per cent of cases and 83.1 per cent of loss values) are committed using the Faster Payments System (UK FPS), illustrating how FPS can become a prime target for Account Push Payment (APP) fraud.[14] Australia's NPP was launched in 2018, and now exceeds 100 million payments each month, which are worth about A$110 billion. Currently, there is no publicly available data regarding the volume of scams and fraud being perpetrated using this payment rail.[15] AusPayNet's member feedback and case studies presented to its Economic Crime Forum point to criminals utilising the NPP and to a majority of cases having a cross-border nexus. According to Westpac Banking Corporation (WBC) data, 45 per cent of their scam recipient accounts have a nexus to the UK.[16]

Domestic FPS allow criminals to launder funds in the same manner as traditional payment rails. Placement and layering of illicit funds occurs via multiple accounts, before integration and then exfiltrating funds internationally via cross-border payments or on alternative money laundering gateways, such as cryptocurrency or money remitters. Often, this process is completed before a target realises they are the victim of a scam. Usage of domestic FPS dramatically increases the speed of the placement, layering and integration stages of the scams and fraud cycle.

The Focus Note published by the World Bank Group's Project FASTT[17] provides a non-exhaustive summary of fraud considerations, viewed through the prism of FPS, in the following table:

[12] UNODC (2024), 'Money laundering'. Available at <https://www.unodc.org/e4j/en/organized-crime/module-4/key-issues/money-laundering.html>.
[13] Also referred to as 'authorised push payment' fraud (APP)
[14] World Bank Group (2023), 'Fraud Risks in Fast Payments', October. Available at <https://fastpayments.worldbank.org/sites/default/files/2023-10/Fraud in Fast Payments_Final.pdf>.
[15] Work is underway with AFCX to determine fraud/scam density by payment rail.
[16] Westpac (2024), 'Stopping scammers before they scam you'. Available at <https://www.westpac.com.au/news/money-matters/2024/08/scams-the-view-from-the-frontline/>.
[17] See World Bank Group (2023)

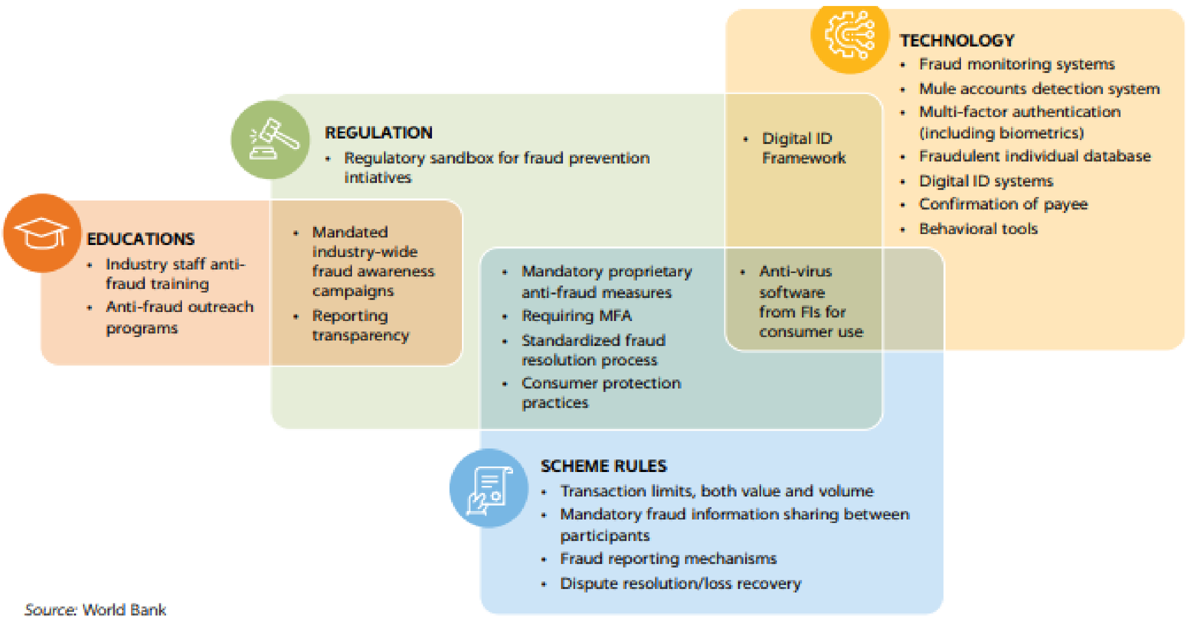


Key Features*	Indicative Benefits	Fraud Considerations
Posting speed	• Funds are available to the beneficiary in seconds. • Funds are sent to a bank account, not to a prepaid/ prefunded instrument that needs to be funded/ defunded.	• Strict service-level agreements based on scheme rules mean that payment service providers and FPS operators have little time to run fraud checks (such as anti-money-laundering or countering the financing of terrorism). • Even if fraud is identified, the time to respond is much shorter because the recipient has immediate access to funds and can move them between many accounts (that is, so-called money mules).
24/7/365 availability	• Continuous system availability mimics features of cash. • Increases utility for the sending and receiving parties.	• Fraudsters can work around the clock and at odd hours, especially when bank staff members are not active. For this reason, victims may not be able to check their accounts and report fraudulent activity to the authorities quickly.
Payment finality	• Provides greater security around the payment because it cannot be reversed. • Helps improve cash flow for companies/merchants. • The lack of chargebacks makes fast payments more attractive than cards in the e-commerce or physical point-of-sale environment.	• Money that is fraudulently stolen from an account cannot be easily reversed, as with a card payment (for example, chargebacks). • By the time a transaction is deemed to have been fraudulent, the illegally obtained funds may already be gone. This can make lost funds very hard to recover.
High transaction limits	• Many FPS have relatively high transaction limits that can support a variety of business use cases. • The higher the limit, the greater the number of use cases that can be supported.	• The ability to send a large amount of money in a single transaction can make fast payments very attractive for fraudsters.

*This list of FPS features is not exhaustive.

Source: World Bank Group; Focus Note Fraud Risks in Fast Payments October 2023

It goes further in advocating a number of potential fraud-mitigating suggestions and solutions that could be included in a payments scheme, such as FPS, as demonstrated in the following illustration:



TECHNOLOGY
- Fraud monitoring systems
- Mule accounts detection system
- Multi-factor authentication (including biometrics)
- Fraudulent individual database
- Digital ID systems
- Confirmation of payee
- Behavioral tools

REGULATION
- Regulatory sandbox for fraud prevention intiatives

- Digital ID Framework

EDUCATIONS
- Industry staff anti-fraud training
- Anti-fraud outreach programs

- Mandated industry-wide fraud awareness campaigns
- Reporting transparency

- Mandatory proprietary anti-fraud measures
- Requiring MFA
- Standardized fraud resolution process
- Consumer protection practices

- Anti-virus software from FIs for consumer use

SCHEME RULES
- Transaction limits, both value and volume
- Mandatory fraud information sharing between participants
- Fraud reporting mechanisms
- Dispute resolution/loss recovery

Source: World Bank

Like many jurisdictions, Australia has seen a rise in both the volume and value of scams perpetrated against its consumers. Because of the volume of scams involving life-changing losses and the difficulty in recouping funds, particularly from offshore jurisdictions, PSPs – including financial institutions – have strongly responded to the threat. Similar to the World Bank's Focus Note, Australian PSPs have implemented several initiatives to rebuild consumer trust and mitigate consumer losses to scams and associated money laundering. Some of these solutions include:

- Confirmation of payee/verification of payee.
- Transaction monitoring and fraud risk scoring powered by machine learning and AI.
- In/out bound account risk scoring.
- First-time payment holds and transaction limits.
- Blocking of high-risk merchants such as digital currency exchanges.
- In the non-bank PSP sector, moving away from pooling funds under a singular account to allow the fraud densities of at-risk merchants to be monitored.
- Developing questions for high-risk transactions to assist the customer and fraud practitioners in identifying suspected scams or money laundering transactions.[18]
- AML/CTF screening.
- Stronger customer onboarding and enhanced customer due diligence via biometric verification.
- In-app verification of One-Time Passcodes and confirmation of caller identities.[19]
- Establishment of Australia's first SMS Sender ID registry[20] to help prevent scammers imitating trusted industry or government brands in text messages.
- Device and behavioural biometrics to mitigate against account takeover, credential selling and mule accounts.
- Enhanced funds tracing and recovery processes via the Australian Financial Crimes Exchange (AFCX) through its Fraud Reporting Exchange (FRX).

These measures have been the major levers, resulting in a 41 per cent reduction in scam losses in Australia over the period July 2023 through end of June 2024.[21] According to WBC data, one in every 25,000 payments is a scam, and they are detecting 69 per cent of all scam attempts, saving customers over A$170 million in 2024.[22] As scams originate on digital platforms and telecommunications services, government initiatives, in the absence of SbD, including the formation of the National Anti-Scam Centre (NASC) and the recently implemented Scam Prevention Framework Bill, will assist in closing the enablers of scams and limiting initial contact with targets, resulting in further reductions. This is a demonstration that retro-fitting solutions can make a material difference and should not be shied away from.

What seems to be missing is a holistic approach to preventing fraud and scams. As an example, the Committee on Payments and Market Infrastructures' (CPMI) '*Principles for financial and market infrastructures*'[23] (PFMIs) apply requirements for the design and management of risk in market infrastructures. Section 1.15 articulates that 'FMIs are to enhance safety and efficiency in payment, clearing, settlement, and recording arrangements,

[18] Westpac, 'Westpac SaferPay'. Available at <https://www.westpac.com.au/security/how-we-protect-you/westpac-saferpay/>.

[19] Sydney Morning Herald (2024), 'Why this bank is moving away from SMS', *Sydney Morning Herald*, 22 October.

[20] ACCC (2024a), 'Targeting scams: Report of the National Anti-Scam Centre on scams activity 2023', April. Available at <https://www.nasc.gov.au/system/files/targeting-scams-report-2023.pdf>.

[21] NASC (National Anti-Scam Centre) (2024), 'National Anti-Scam Centre in action: Quarterly update (April to June 2024)', November. Available at <https://www.nasc.gov.au/reports-and-publications/quarterly-update/nasc-quarterly-update-april-june-2024>.

[22] See Westpac (2024)

[23] BIS (Bank for International Settlements) (2012), 'Principles for financial market infrastructures', April. Available at <https://www.bis.org/cpmi/publ/d101a.pdf>.

and more broadly, to limit systemic risk and foster transparency and financial stability.' As has already been highlighted, the growth in fraud and scams globally suggest that the PFMIs should be updated to reflect the growing threat of these activities and their role in undermining confidence in the digital economy. This is particularly relevant given that many FPS could be classified as systemically important payment systems.

In its *Final report to the G20: Linking fast payment systems across borders: governance and oversight*',[24] CPMI notes that fraud risk requires special attention, with some suggestion of the usage of 'transaction screening and text message alerts for users'.[25] However, in its article '*Fast Payments: design and adoption' (2024 Frost et al), in the March edition of the BIS Quarterly Review',*[26] there is no mention of fraud risk in terms of the design factors.

Similar to other 'by design' frameworks, such as 'Privacy by Design' and 'Security by Design', SbD offers a holistic framework that may assist in optimising the approach that PSPs and PSOs take to product and platform design, as well as the implementation of new payment platforms to mitigate the risk of fraud and scams. Its application to legacy and new payment platforms by PSOs and PSPs will deliver better outcomes for both users and service providers, while ensuring trust and confidence in the ecosystem.

Safety by Design (SbD)

SbD encourages a design ethos that embeds risk mitigation and user protections during product development, as well as post-implementation for all actors in the digital ecosystem (i.e. digital marketplaces, telecom companies). As such, it is argued that the SbD Principles developed by the Office of the eSafety Commissioner[27] in Australia are also well suited for incorporation by PSPs and PSOs into their design philosophy.

These principles are as follows:

1. Service provider responsibility
2. User empowerment and autonomy
3. Transparency and accountability

These principles should form the foundation by which PSPs and PSOs deliver payments products. The SbD Principles are set out in full in **Appendixes 1-3**. This paper will categorise, explore and make recommendations based on the SbD Principles.

Principle 1: Service provider responsibility

Central to this principle is that the burden of safety should never fall solely on the end-user and that service providers should take preventative steps to ensure that their service is less susceptible to facilitating harms, fraud, scams or other illegal or inappropriate behaviours. The full suite of steps within this principle are set out in **Appendix 1**.

To that end, best practices are emerging to mitigate a range of issues that PSPs and PSOs are experiencing and that can arise on both legacy and newer digital platforms. These best

[24] BIS (2024*), '*Final report to the G20: Linking fast payment systems across borders: governance and oversight', October. Available at <https://www.bis.org/cpmi/publ/d223.pdf>.
[25] See BIS (2024)
[26] Frost J, Koo Wilkens P, Kosse A, Shreeti V, Velasquez C (2024), 'Fast payments: design and adoption', *BIS Quarterly Review, March,* pp 31-44. Available at <https://www.bis.org/publ/qtrpdf/r_qt2403c.pdf>.
[27] eSafety Commissioner (2024), 'Safety by Design'. Available at <https://www.esafety.gov.au/industry/safety-by-design>.

practices can be generally categorised as risk-based frictions. While it essentially goes against the generalised model of fast and frictionless payments, a significant lever has been the introduction of appropriate risk-based frictions in slowing the authorisation of real-time payments under certain circumstances. Indeed, the Australian Government articulated this point in '*A Strategic Plan for Australia's Payments System*',[28] in which it outlined that maintaining 'intelligent friction' to improve the trustworthiness in a system (such as deliberately slowing down payments to increase security checks within a transaction) may be desirable, and that any resultant reduction in efficiency would be appropriate in the circumstances.[29.]

The following are examples of intelligent frictions for consideration by PSPs and PSOs that may assist in reducing harms, fraud, scams and other illegal or inappropriate behaviours.

Risk scoring

An example of risk scoring is the decision to hold or block payments. Such decisions are often based on internal fraud systems that analyse observable data, transaction patterns, and fraud rules and are powered via device biometrics and machine learning. In Australia, the sharing of risk scoring via an Application Programming Interface (API) to both the sending and receiving accounts is an important metric to determine whether a payment should be held or blocked.[30] In an interlinked FPS context, consideration can be given to:

- Allowing a risk score to be shared between a sending and receiving PSP.
- Allowing each PSP to consider the risk score, in addition to their internal information, to inform any payment hold, block or supporting transaction questions.
- Sharing a standardised risk score via technologies such as API, which allows for interoperability between different fraud monitoring products, that in turn promotes competition, inclusion and data security.

We note that there may be data privacy considerations in any cross-border approach, and thus, any cross-border transmission of data needs to be carefully evaluated. The complexity of this approach is recognised, yet the results are promising. Onerous blocking or holding of payments can, however, adversely impact supply chains, investments and home purchases. In Australia, determining appropriate payment holds has required PSPs to carefully ascertain the appropriate balance between risk-based frictions and false positives on genuine transactions, so as not to impact the economy disproportionately. Blocking of high-risk merchants, such as non-compliant digital currency exchanges, is also a vector for PSPs to consider. For cross-border payments, risk scoring would need to consider, as an example, that an established multinational company sending payments to a historical recipient may be a low risk, compared to a newly established small business sending a first-time payment. Proportionality would need to be applied in this example.

Transaction limits

The G20 has been pursuing a *Roadmap for Enhancing Cross-border Payments*, which focuses on reducing the cost and enhancing the speed, access, and transparency of payments across borders. This is a significant driver for interlinking domestic FPS for cross-border payments. The G20's push for real-time payments, largely driven by economic benefits, did not anticipate how rapidly organised crime could exploit this speed for rapid money

[28] Australian Government (2023), 'A Strategic Plan for Australia's Payments System', June. Available at <https://treasury.gov.au/sites/default/files/2023-06/p2023-404960.pdf>.

[29] See Australian Government (2023)

[30] Musat I (2024), 'Australian banks team up with BioCatch to mitigate fraud and scams', *The Paypers,* 25 November. Available at <https://thepaypers.com/fraud-and-fincrime/news/australian-banks-team-up-with-biocatch-to-mitigate-fraud-and-scams>.

laundering,[31] largely leaving this responsibility to PSPs and PSOs to manage. Consequently, a lesson from domestic FPS is that PSPs should consider risk-based transaction limits for FPS interlinked for cross-border payments and also consider implementing first-time payment holds. These have emerged as key features of the Australian domestic FPS to reduce the risk of fraudulent and mistaken payments. As such, they also apply to account-to-account cross-border payments using interlinked FPS. The rationale is that embedding intelligent frictions prior to a payment being cleared and settled irrevocably in real-time reduces the significant effort involved in recovering and repatriating funds. Fundamentally, prevention is better than cure, and never has the need for such prevention been greater.

Fraud Data Exchange

The AFCX developed the FRX in 2023. The FRX provides a platform for PSPs and other participants to securely and efficiently share information on fraudulent payments in near-real time, to assist with loss prevention and recovery efforts. Under the Scam-Safe Accord, all Australian Banking Association (ABA) and Customer Owned Banking Association (COBA) members – together 73 financial institutions – will join the FRX by mid-2025. Importantly, several cryptocurrency exchanges have also joined the FRX, enabling direct communication and collaboration with PSPs to trace and recoup fraudulent funds transferred to those exchanges, and facilitating a whole of ecosystem approach. This becomes increasingly important as funds are often hopped via real-time payments between mule accounts and exit the regulated system via cryptocurrency. As FPS become interconnected for cross-border payments, consideration will need to be given to ways of improving funds tracing and recovery.

PSPs and PSOs will need to continue collaborating on creating an environment that prevents criminals from accessing payment rails. With the emergence of national anti-scam centres in many jurisdictions, there may be an opportunity to leverage these capabilities. However, this may require inter-governmental engagement to overcome legal obstacles to enhanced data sharing between jurisdictions.

Enhanced Know Your Customer (KYC) and customer due diligence

The bedrock of confidence and trust is ensuring that strong customer onboarding and enhanced customer due diligence processes are undertaken. With increasing data theft occurrences, biometric verification methods are now essential to confirm the identity of the person producing documents when opening accounts online, or confirming the entity operating an account digitally when banks suspect an account has been taken over or subject to credential on-selling.[32] These key risk mitigation measures were recognised domestically in the Australian Scam Safe Accord.[33]

Additional Technical Features

Australia's first SMS Sender ID registry to help prevent scammers from imitating trusted industry or government brands in text messages[34] is being established, after legislation was passed by the Australian Government in August 2024, and is expected to be fully operational by December 2025. This was in response to criminals using publicly available technology to

[31] The Payments Association (2024), 'The impact of APP fraud on cross-border payments', Whitepaper. Available at <https://thepaymentsassociation.org/whitepaper/the-impact-of-app-fraud-on-cross-border-payments/>.

[32] See Westpac (2024)

[33] ABA (Australian Banking Association), 'Keeping Australia Scam Safe'. Available at <https://www.ausbanking.org.au/scam-safe-accord/>.

[34] Rowland M (2024), 'Better protections for Australians from SMS scams', Media Release, 3 December. Available at <https://minister.infrastructure.gov.au/rowland/media-release/better-protections-australians-sms-scams>.

infiltrate the text message feeds of banks and other businesses. It was particularly problematic for banks as it enabled criminals to conduct high-value bank impersonation scams. Banks have continued gravitating to issuing communications, one-time-passcodes and other customer notifications within their digital banking application (mobile app). The in-app verification is supported in the background by biometric device technologies, enabling greater security to mitigate credential takeover and even enabling the banks and customers to confirm each other's identity when communicating online or via a call centre.

Principle 2: User empowerment and autonomy

The steps in this principle promote the inclusion of tools and technical features to mitigate risk and harms which can be flagged to users. Moreover, it promotes a design process that incorporates self-evaluation to ensure risk factors are mitigated before products or services are released. The full suite of considerations for Principle 2 are set out in **Appendix 2**.

Confirmation of Payee

Confirmation of Payee (CoP) is an account name verification service that effectively validates account names before payment initiation.[35] CoP systems have been developed to support domestic payment systems globally, including the UK, Europe and now Australia and New Zealand. The UK Payments Association notes that CoP has led to enhanced confidence in UK domestic payments by ensuring funds are directed to the intended account holder. The service is also useful to customers making payments to unfamiliar accounts, in reinforcing the overall reliability of financial transactions and reducing the risk of errors.[36]

CoP is not a panacea for mitigating all scams; it helps to mitigate some scams, such as false invoice or bank term deposit scams; however, social engineering by criminals often explains away name discrepancies. Due to the challenges of tracing and recalling mistaken payments, CoP has become a key customer experience feature in preventing mistaken payments, especially when making large account-to-account payments. Internationally, 72 per cent of Swift payments requiring manual interventions are the result of avoidable mistaken payment errors.[37] It is a similar scenario domestically, with data released by the Commonwealth Bank of Australia (CBA) showing that their CoP solution ('NameCheck') has prevented more than A$370 million in mistaken payments and A$40 million in scam losses.

To support the prevention of scams and ensure compliance with AML/CTF requirements, AusPayNet members' view is that the effectiveness of name-checking technologies is significantly enhanced when used in conjunction with observable transaction data. This integrated approach enables more accurate risk scoring to determine whether a payment should be held, particularly in instances where customers can be asked for further information regarding the purpose of the transaction. While many PSPs have internal fraud solutions to develop risk scoring that assists in payment holds, WBC has developed technology that requires identified at-risk transactions to be strengthened with additional customer questions before authorisation. This not only improves the risk score but assists the customer in pausing

[35] ABA (2024), 'New Confirmation of Payee service hits important milestone', Media Release, 8 August. Available at <https://www.ausbanking.org.au/new-confirmation-of-payee-service-hits-important-milestone/>; AP+ (Australian Payments Plus) (2023), 'Development of industry Confirmation of Payee Solution', Media Release, 30 November. Available at <https://www.auspayplus.com.au/development-of-industry-confirmation-of-payee-solution>.

[36] Chakraborty R (2024), 'Understanding confirmation of Payee: The route to enhanced security in payment services', The Payments Association, 28 February. Available at <https://thepaymentsassociation.org/article/understanding-confirmation-of-payee-the-route-to-enhanced-security-in-payment-services/>.

[37] Swift (2023), 'Taking local Confirmation of Payee global', September. Available at <https://www.swift.com/news-events/news/taking-local-confirmation-payee-global>.

and questioning the legitimacy of the payment. As of August 2024, WBC had challenged 200,000 payments, resulting in A$194 million in abandoned payments.[38] The WBC solution ('Verify') has led to a reduction in business email compromise scams but, importantly, is also stopping 300 mistaken payments a day.[39]

As the world moves to fast cross-border payments, the European Commission has recognised the need to mandate the pre-validation of accounts to mitigate fraud and mistaken payment losses on cross-border payments.[40] Similarly, Swift's pre-validation solution allows integration into domestic CoP solutions and communication via APIs to avoid data privacy constraints.[41] Swift has retro-fitted this to their existing cross-border payment rail. This approach provides its members a lower-cost mechanism for addressing the threat of scams.

CoP has demonstrably improved the customer experience and empowered users to confidently send payments to their intended beneficiaries. Its extension into cross-border payments will deliver the same benefits. As a proven tool, it should be included in the toolkit of all payment systems, including FPS, irrespective of whether they interlink for cross-border payments. Nonetheless, there are challenges concerning data privacy when it comes to cross-border payments. Overall, PSOs and PSPs should be cognisant of these challenges and pursue CoP models that deliver the same outcomes as domestic CoP, namely enhanced user experience and the ability to deliver a payment to its intended beneficiary.

Principle 3: Transparency and accountability

The full suite of steps and considerations for Principle 3, Transparency and accountability are detailed in **Appendix 3**.

This principle promotes a culture of embedding end-user safety. This may include appropriate levels of staff training and practices into staff training to embed that culture. It further promotes transparency, not just for the end-user but in terms of publishing metrics to the extent of the performance of products against the safety objectives. It further promotes a culture of continuous improvement. As a matter of course, transparency as to the success of efforts in mitigating financial crime is in everybody's interest, as is the communication of those strategies that are effective. Sharing of best practice processes as well as technologies has been demonstrated to yield positive results. Examples could include the sharing of mule account information, algorithms that have been developed to detect sexploitation and collaborating with law enforcement and others on targeting new typologies. The culture of continuous improvement and collaboration across the ecosystem, from financial institutions to telecommunication providers, has defined the Australian success story in developing and sharing risk mitigants, without which success would be inconceivable. However, the next phase is for this to occur globally.

[38] See Westpac (2024)
[39] See Westpac (2024)
[40] Regulation (EU) 2024/886 of the European Parliament and of the Council
[41] See Swift (2023)

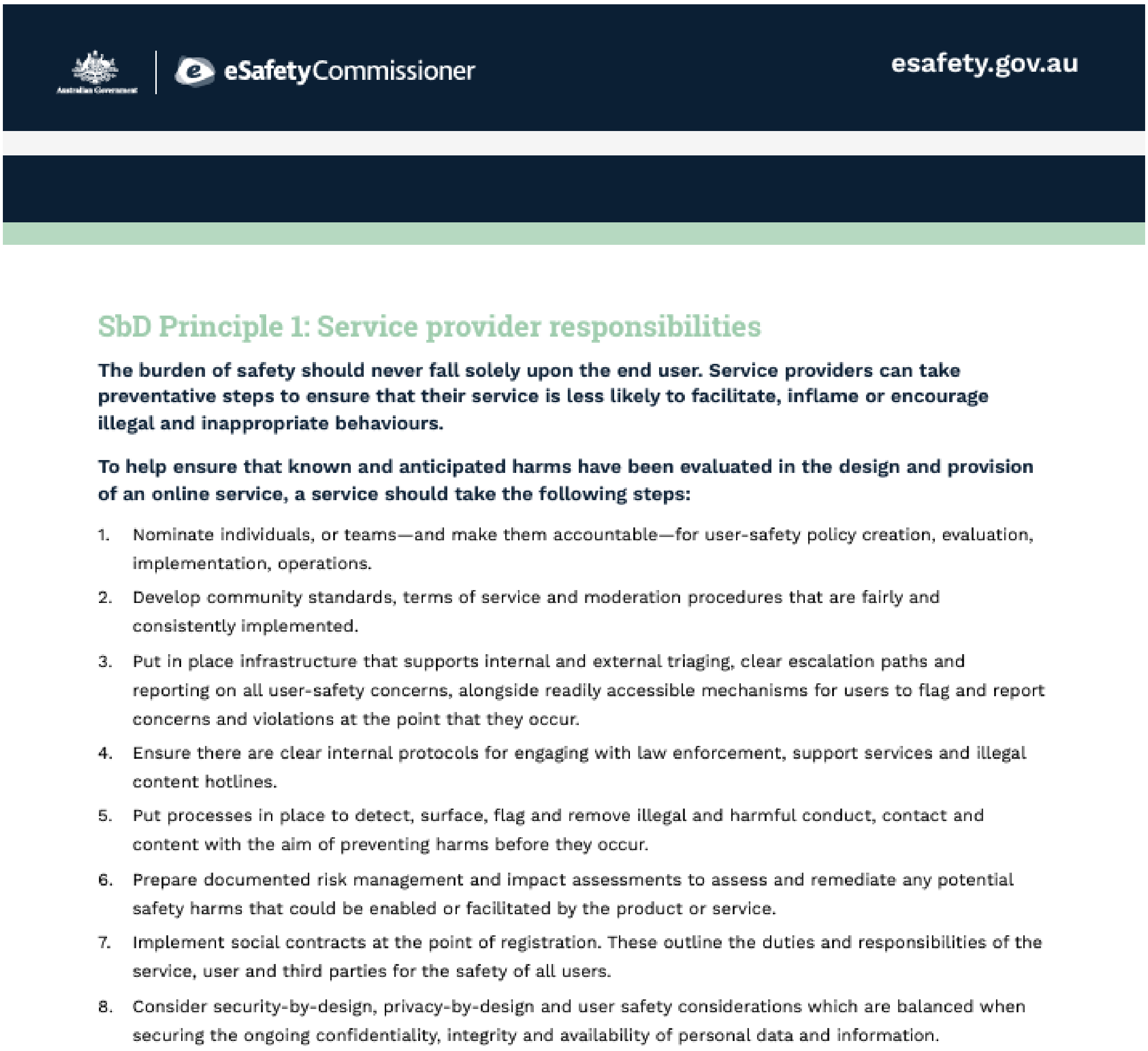
Recommendations

We recommend that supra-national bodies, such as CPMI and the FSB, re-assess the impact of scams and fraud on the digital economy. Moreover, they should take steps to support and galvanise an ecosystem wide approach to tackling this threat globally. Alongside speed, access, transparency and cost, safety is also an important factor in cross-border payments. To avoid the irreparable erosion of consumer confidence in the digital economy, the FSB and CPMI, in conjunction with other bodies, should promote the use of SbD.

National authorities should also encourage the adoption of SbD within their payment system ecosystem by PSPs and PSOs, recognising that every payments ecosystem is unique in its architecture. That may mean that SbD is adopted to the extent that is possible by each stakeholder within their respective payments ecosystem.

Appendix

Appendix 1 – Service provider responsibility



Australian Government | eSafetyCommissioner

esafety.gov.au

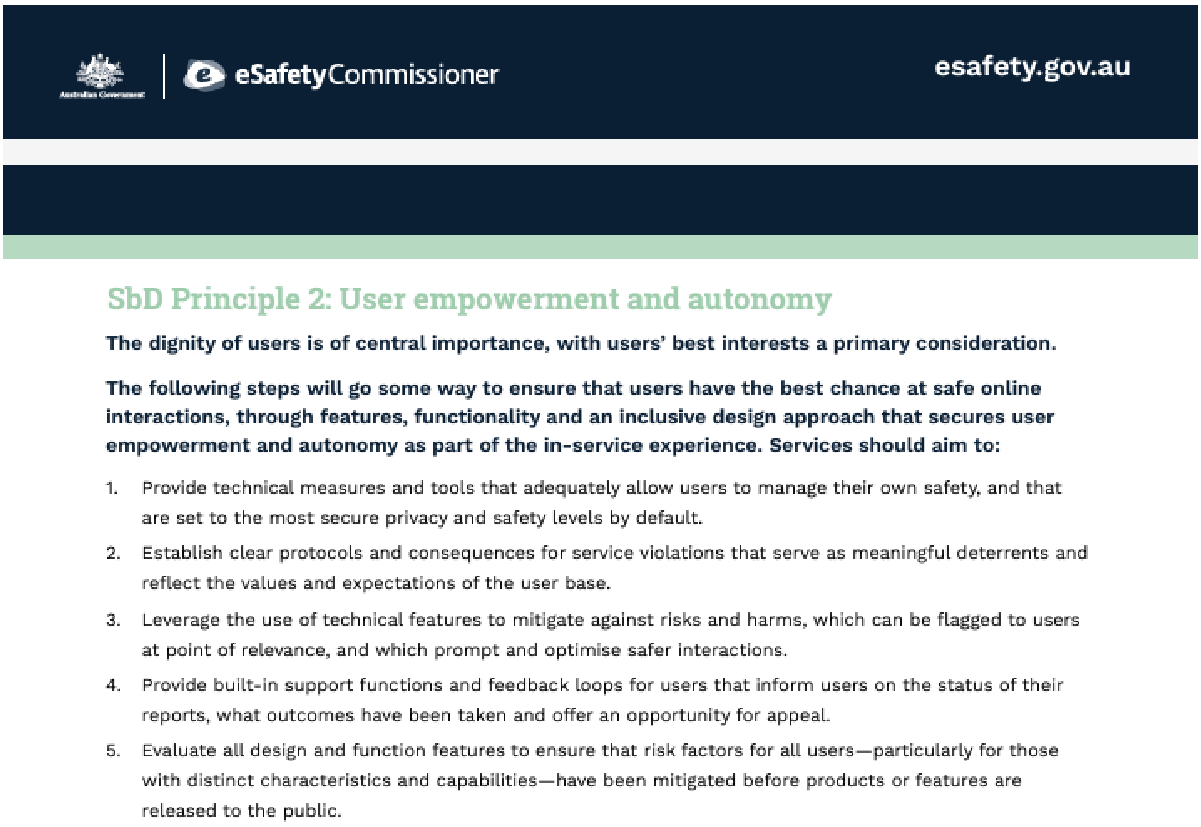
SbD Principle 1: Service provider responsibilities

The burden of safety should never fall solely upon the end user. Service providers can take preventative steps to ensure that their service is less likely to facilitate, inflame or encourage illegal and inappropriate behaviours.

To help ensure that known and anticipated harms have been evaluated in the design and provision of an online service, a service should take the following steps:

1. Nominate individuals, or teams—and make them accountable—for user-safety policy creation, evaluation, implementation, operations.
2. Develop community standards, terms of service and moderation procedures that are fairly and consistently implemented.
3. Put in place infrastructure that supports internal and external triaging, clear escalation paths and reporting on all user-safety concerns, alongside readily accessible mechanisms for users to flag and report concerns and violations at the point that they occur.
4. Ensure there are clear internal protocols for engaging with law enforcement, support services and illegal content hotlines.
5. Put processes in place to detect, surface, flag and remove illegal and harmful conduct, contact and content with the aim of preventing harms before they occur.
6. Prepare documented risk management and impact assessments to assess and remediate any potential safety harms that could be enabled or facilitated by the product or service.
7. Implement social contracts at the point of registration. These outline the duties and responsibilities of the service, user and third parties for the safety of all users.
8. Consider security-by-design, privacy-by-design and user safety considerations which are balanced when securing the ongoing confidentiality, integrity and availability of personal data and information.

Appendix 2 - User empowerment and autonomy



eSafetyCommissioner

esafety.gov.au

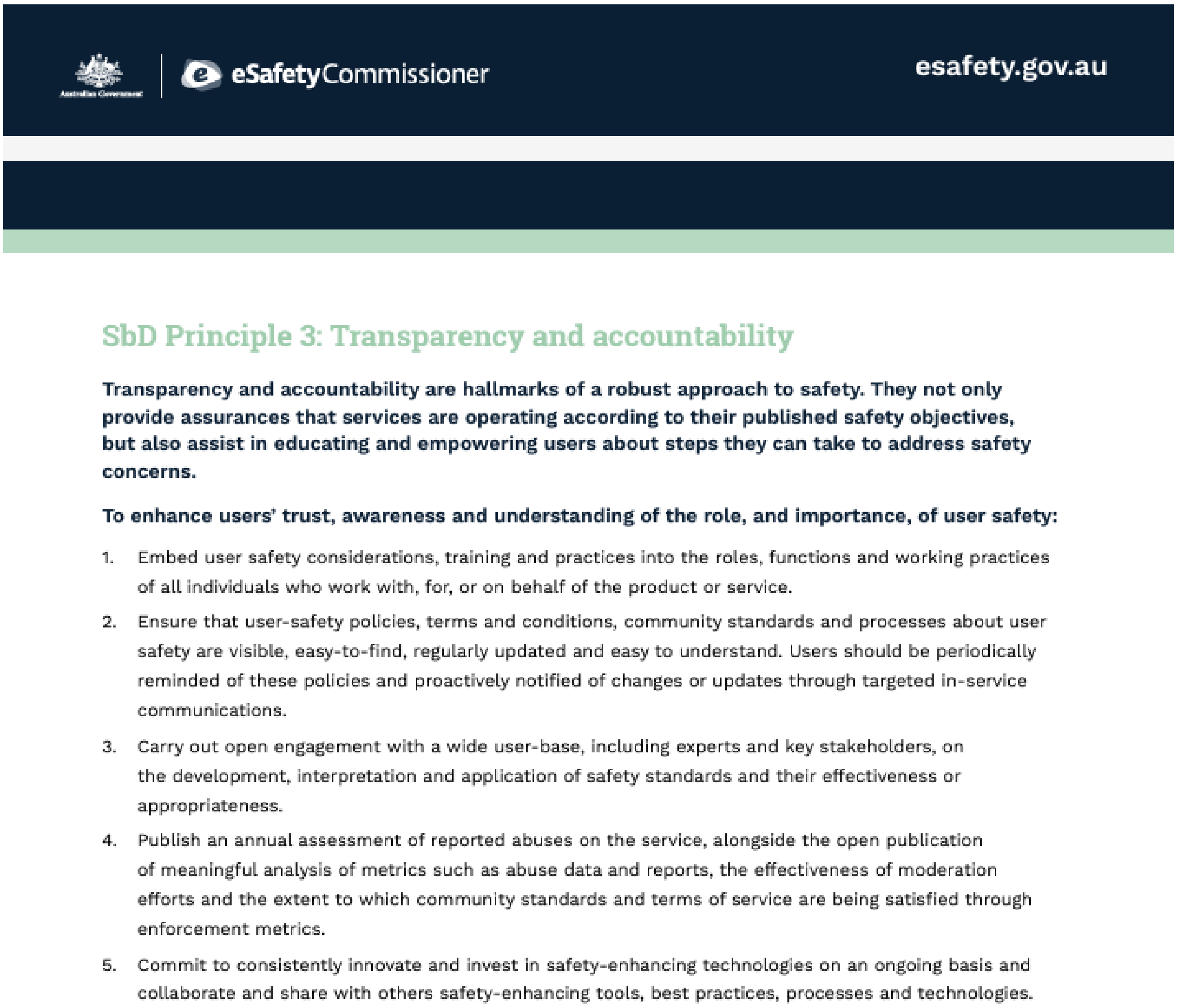
SbD Principle 2: User empowerment and autonomy

The dignity of users is of central importance, with users' best interests a primary consideration.

The following steps will go some way to ensure that users have the best chance at safe online interactions, through features, functionality and an inclusive design approach that secures user empowerment and autonomy as part of the in-service experience. Services should aim to:

1. Provide technical measures and tools that adequately allow users to manage their own safety, and that are set to the most secure privacy and safety levels by default.
2. Establish clear protocols and consequences for service violations that serve as meaningful deterrents and reflect the values and expectations of the user base.
3. Leverage the use of technical features to mitigate against risks and harms, which can be flagged to users at point of relevance, and which prompt and optimise safer interactions.
4. Provide built-in support functions and feedback loops for users that inform users on the status of their reports, what outcomes have been taken and offer an opportunity for appeal.
5. Evaluate all design and function features to ensure that risk factors for all users—particularly for those with distinct characteristics and capabilities—have been mitigated before products or features are released to the public.

Appendix 3 – Transparency and accountability



Australian Government | eSafetyCommissioner

esafety.gov.au

SbD Principle 3: Transparency and accountability

Transparency and accountability are hallmarks of a robust approach to safety. They not only provide assurances that services are operating according to their published safety objectives, but also assist in educating and empowering users about steps they can take to address safety concerns.

To enhance users' trust, awareness and understanding of the role, and importance, of user safety:

1. Embed user safety considerations, training and practices into the roles, functions and working practices of all individuals who work with, for, or on behalf of the product or service.
2. Ensure that user-safety policies, terms and conditions, community standards and processes about user safety are visible, easy-to-find, regularly updated and easy to understand. Users should be periodically reminded of these policies and proactively notified of changes or updates through targeted in-service communications.
3. Carry out open engagement with a wide user-base, including experts and key stakeholders, on the development, interpretation and application of safety standards and their effectiveness or appropriateness.
4. Publish an annual assessment of reported abuses on the service, alongside the open publication of meaningful analysis of metrics such as abuse data and reports, the effectiveness of moderation efforts and the extent to which community standards and terms of service are being satisfied through enforcement metrics.
5. Commit to consistently innovate and invest in safety-enhancing technologies on an ongoing basis and collaborate and share with others safety-enhancing tools, best practices, processes and technologies.