## AUSPAYNET INSIGHTS PAPER:

# ARTIFICIAL INTELLIGENCE IN PAYMENTS

Artificial Intelligence (AI) has the potential to deliver significant benefits across many areas of the global economy and society. This has long been recognised by the payments industry, which has been integrating AI into systems and processes for many years to help drive efficiency, security, and innovation.

As AI models become more sophisticated in their ability to process vast amounts of data, recognise complex patterns, and generate intelligent insights, the potential applications of this technology within the payments ecosystem also continue to evolve. These include further enhancing fraud detection and risk management capabilities, improving operational efficiency and resilience, and supporting innovation and improvements in payments technologies and services, including through more personalised customer and merchant experiences.

However, a number of risks and challenges stand in the industry's way of realising the full potential of AI. The integration of AI requires significant investments in data, infrastructure and talent, which can present barriers to adoption, especially for smaller players.

Important concerns have also been raised around the safe and ethical implementation of AI systems, with issues such as data privacy, model risk, security and accountability requiring careful consideration and management by entities adopting these technologies. Regulatory uncertainty surrounding the use of AI in financial services also adds complexity, with continued collaboration between industry stakeholders and policymakers necessary to ensure clarity of regulatory obligations and the establishment of appropriate governance frameworks that foster innovation while protecting consumer interests.

This paper presents insights on some of the key opportunities presented by ongoing advancements in AI capabilities for the payments industry, focusing on applications that would be expected to provide the most benefit at an ecosystem level. The paper then examines the key barriers to realising these opportunities, and provides recommendations for how the industry can work together to overcome these challenges for the benefit of all ecosystem participants and its end users.

# THE OPPORTUNITIES

Recent advances in AI are creating unprecedented possibilities for enhancing the safety, efficiency and resilience of payment systems. This section explores some of the most promising applications of AI technology for addressing longstanding challenges in the payments ecosystem, focusing on opportunities that could deliver significant benefits at an industry-wide level.

## OPPORTUNITY 1: COMBATTING ECONOMIC CRIME

### Current landscape

The marked shift towards digital and increasingly real-time payment methods over the past decade has been accompanied by a significant rise in economic crime. In 2023, the value of payment card fraud in Australia increased to $762 million, and the value of reported scams to over $2.7 billion – a 325 per cent increase since 2019.[1] Globally, it is estimated that 2-5 per cent of global GDP, or up to US$2 trillion, is laundered each year.[2] This is costly not just for the individuals and businesses directly affected by such criminal activity, but also for the financial institutions through which this activity occurs, with the estimated global cost of financial crime compliance amounting to around $200 billion in 2023.[3]

Payment service providers (PSPs) have been leveraging Machine Learning (ML) as part of their fraud management toolkit for many years, given its ability to analyse large data sets, identify patterns and anomalies, and adapt to new information over time.[4] Unfortunately, AI is also increasingly being exploited by criminal actors to amplify the scale and sophistication of their activities. The public availability of advanced Generative AI (GenAI) tools in particular has enabled criminals to generate more convincing phishing attacks, create realistic fake documents and identities, better impersonate their targets' biometric traits, and write more effective malware code to automate fraudulent attacks. Developments in AI capabilities such as Adversarial ML are also helping criminals bypass banks' security measures and evade traditional rules-based detection methods. Moreover, the widespread availability of such AI tools means that these techniques are no longer limited to only the more sophisticated criminals. This all means that not only is there a rapidly growing volume of criminal activity, but it is also becoming harder to detect.

As the scale and complexity of economic crime continue to increase, banks will need to continuously enhance their fraud detection tools to keep pace. Currently, many fraud detection systems used by PSPs continue to rely on fairly static and reactionary rule sets. By their nature, ML algorithms iteratively learn from new information, and can therefore help identify evolving fraud patterns and improve their accuracy over time. However, most PSPs do not currently allow for automatic updates to their fraud systems, and instead rely on infrequent human action to validate and adopt any AI-identified changes to the rule set. Many fraud systems also group customers together into large population segments based on certain high-level attributes. Anomalies are identified by comparing each customer's transaction against the 'normal' behaviour of their population, rather than the individual traits of that customer. Such limitations can reduce the effectiveness of fraud detection systems, increasing the likelihood of both false negatives (fraudulent transactions that are allowed to proceed) and false positives (incorrectly declined transactions), both of which can be a significant cost for businesses.

[1] Australian Payments Network (2024), *Australian Payment Fraud 2024*, 25 September; Australian Competition and Consumer Commission (ACCC) (2024), *Targeting scams: Report of the ACCC on scams activity 2023*, 28 April.

[2] United Nations, *Money Laundering: Overview*, accessed September 2024.

[3] LexisNexis (2023), *True Cost of Financial Crime Compliance Study 2023*, 26 September.

[4] For the purposes of this paper, the term 'PSP' is intended to capture all providers of payments services in the ecosystem, including payment system operators, financial institutions, payments technology providers, and payments fintechs.

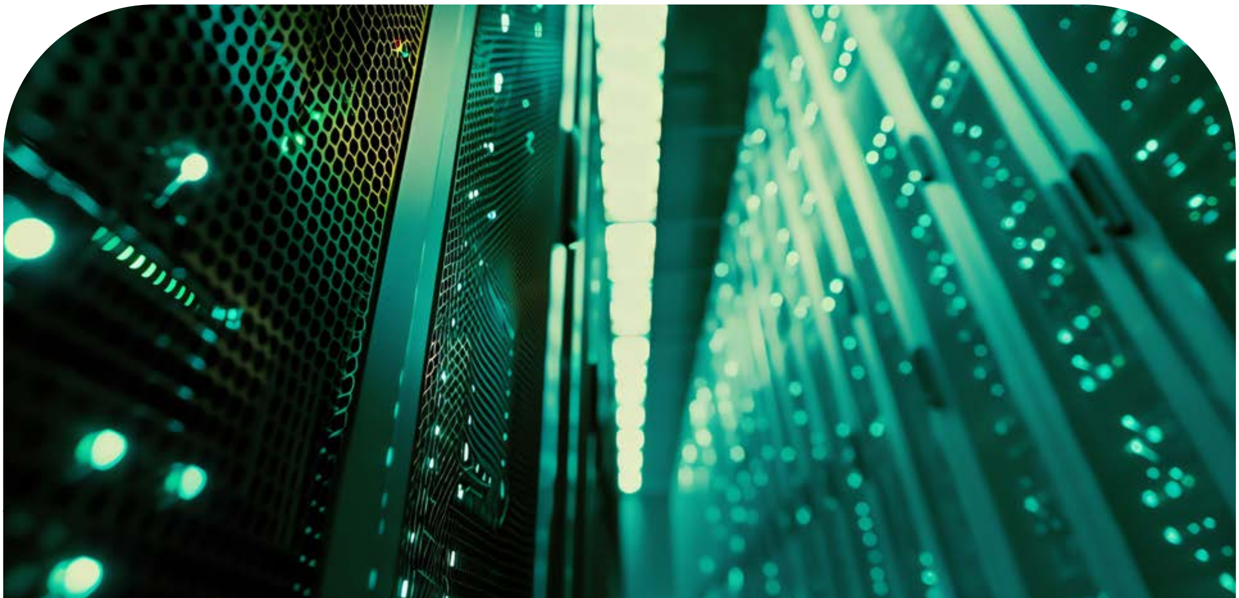
## Potential developments

Ongoing developments in AI technology provide significant opportunities for PSPs to enhance their fraud detection capabilities. These opportunities include:

- **Enhanced accuracy:** Deep learning model capabilities can be used to integrate and derive insights from a much wider range of both structured and unstructured data sources. Such sources could include customer profiles, transaction histories, cross-channel activity, behavioural analytics, dark web monitoring, industry intelligence, and market trends. By detecting non-linear relationships between diverse data points, newer AI models can build up a more comprehensive and proactive view of potential fraud risks. Importantly, this could also enable fraud monitoring to occur at the individual customer level, rather than relying on generic rules applying to larger population sets. This would be expected to improve the accuracy of fraud detection, reducing both false positives and false negatives.
- **Enhanced authentication:** AI-supported biometric recognition is already being widely used to authenticate mobile and online payments. Ongoing developments in AI are enabling increased accuracy and performance of biometric authentication tools, which should support more robust identity verification and fraud monitoring. This will become increasingly important as the sophistication of fraudulent activity, including identity theft and presentation attacks, continues to escalate.
- **Enhanced efficiency:** As AI-enabled fraud detection tools become more accurate and reliable, there will be greater scope to allow the systems to continuously adapt to changes in customer behaviour and evolving fraud patterns without the need for human approval of every rule change. There will also be a reduced need for human decisioning on every flagged transaction, which should greatly speed up PSPs' ability to respond to individual instances of potential fraudulent activity. This will be particularly important as more account-to-account transactions move to the real-time payment system. Where human decisioning is required, GenAI techniques could be used to help interpret and provide guidance on a given fraud alert, improving both the speed of investigation and the transparency of the AI system.

Focusing further on GenAI specifically, this technology could also assist PSPs in improving their fraud detection through opportunities such as:

- **Synthetic data augmentation:** GenAI tools could be used to create synthetic data that mimics real-world fraud scenarios to help overcome the challenges of limited data availability, allowing for more robust training and testing of fraud detection systems.
- **Adversarial learning:** GenAI could be used to simulate potential fraud attempts by creating adversarial examples that aim to bypass existing fraud detection systems. This would allow PSPs to be more proactive in identifying and addressing vulnerabilities in their models, and adapting to emerging threats and possible future threat vectors.
- **Explainability:** Certain GenAI models, such as Variational Autoencoders, could be leveraged to provide simple representations of the patterns and decision-making processes learned by an AI model. This can enhance the explainability of fraud detection tools, increasing transparency and trust in their outputs.



### Collaborative analytics

All else equal, the more quality data that is made available for training an AI model, the greater the level of accuracy and output quality it can achieve. This poses challenges for smaller participants in particular, as they have a smaller volume of payments data available for training any bespoke AI systems and must therefore often rely on external tools. However, even larger participants can only see a portion of the transactions in each payment network. In the case of distributed payment systems, such as the account-to-account transfer systems in Australia, even the system operator may not always have full end-to-end network visibility.

With the growing complexity in scams, fraud and money laundering – which often involve moving funds through multiple financial institutions and payment networks to avoid detection – sharing information both within and between PSPs is becoming increasingly important for identifying criminal activity. Pooling payments data across institutions, in compliance with relevant laws and regulatory obligations, could enable AI systems to identify suspicious activities or trends that might otherwise go undetected by individual institutions. In addition to better detecting criminal activity and safeguarding customers, the inclusion of smaller PSPs in collaborative analytics initiatives could help level the playing field across the industry, reducing vulnerabilities and creating a more robust fraud prevention ecosystem.

The potential benefits of collaborative analytics have generated significant attention globally in the past few years. Several information-sharing utilities aimed at combatting economic crime have already been established around the world, including the Monetary Authority of Singapore's COSMIC platform, TMNL in the Netherlands, and the TriBank pilot in the UK. In Australia, initiatives such as the Australian Financial Crimes Exchange (AFCX) and the planned National Anti-Scam Centre (NASC) intelligence-sharing arrangements will also go some way towards better identifying developments in criminal activity across the industry. However, under the AFCX and anticipated NASC models, only information about criminal activity that individual participants have already detected or suspected is shared. This approach therefore still relies on those entities' siloed fraud detection systems, and does not achieve the type of outcomes envisaged under a true collaborative analytics approach. Expanding these initiatives to enable AI-powered collaborative analytics across all transactions in the ecosystem could greatly assist the industry's efforts in the fight against economic crime.

The value of system-wide data has also been recognised by Australian Payments Plus (AP+), which operates the domestic fast payment system, the New Payments Platform (NPP). While the NPP was designed as a distributed system, AP+ is undertaking system developments aimed at providing it with enhanced visibility of transactions across the network, to enable more effective analysis, reporting and potentially prevention of fraud across the system.

## OPPORTUNITY 2: OPERATIONAL RESILIENCE

As payments have become increasingly digital and the payments ecosystem more interconnected, payments system resilience has become more important than ever. Operational outages and cyberattacks can cause significant disruption and cost to the economy, particularly when an incident at one entity has flow-on effects for other PSPs. Due to the potential systemic and customer impacts of operational disruptions in the payments ecosystem, the Reserve Bank of Australia (RBA), Treasury and other financial services regulators have all highlighted system resilience as a key strategic priority for the industry.

Concerningly, the frequency of both operational outages and cyberattacks has been rising in recent years. As in the case of fraud, AI can simultaneously assist PSPs in mitigating these risks, and heighten the threats they face. Improved access to AI technology is expected to increase the sophistication, volume and effectiveness of cyberattacks in particular in the coming years. One study estimates that cybercrime cost the global economy US$8 trillion in 2023, and forecasts the number will rise to $10.5 trillion by 2025.[5] RBA data also show that the frequency and duration of operational outages across retail payment systems has increased in recent years.[6] The effective use of more advanced AI capabilities could help PSPs mitigate these rising risks through enhanced prevention, detection and recovery from operational disruptions, as discussed below.

### Prevention

AI systems could be used to enable smart routing capabilities that not only increase the efficiency of payments processing, but also reduce the risk of operational failures due to system overload and minimise the flow-on impacts of any operational issues on other parts of the network. Currently, payments are often processed based on a series of static rules. AI could optimise payments processing by

[5] Esentire (2024), *2023 Official Cybercrime Report*.

[6] Bullock M (2023), *Modernising Australia's Payments System*, Speech at the AusPayNet Summit, 12 December.

monitoring traffic loads and other operational information across networks in real time, and proactively re-routing transaction pathways based on factors such as speed, capacity and reliability.

AI could also be used to dynamically adjust system parameters and configurations to enhance reliability and performance. This capability could be utilised both within individual PSPs and across a payments network. For example, in line with the Government's *Strategic Plan for Australia's Payments System*, the industry is currently transitioning away from the Bulk Electronic Clearing System (BECS) to more modern payment alternatives, including the NPP. One concern raised by industry participants around the migration of payments to the NPP – which processes payments on a line-by-line rather than a batch basis – is how to efficiently process bulk payments and ensure that the NPP and its participants have sufficient processing capacity to handle the uneven flow of bulk transaction requests throughout the day. While the industry is already preparing for larger payment files to be processed via the NPP, AI could further assist by enabling intelligent capacity throttling to mitigate the risk of any operational issues that may arise.

AI-driven tools could also provide enhanced threat intelligence and predictive analytics. For example, AI could be used to simulate and analyse potential attack paths within a system, and continuously scan for any vulnerabilities across a PSP's systems, ensuring ongoing protection and reducing reliance on infrequent penetration testing. Where vulnerabilities are identified, GenAI tools could be used to recommend fixes or propose mitigation measures.

## Detection

While AI is already commonly used in the detection of operational and cybersecurity issues, increased adoption and ongoing developments in AI technology could lead to a significant further uplift in these capabilities. By better integrating and analysing data from various sources, AI can provide enhanced end-to-end visibility across systems and networks, and assist in more quickly and effectively identifying issues. Unlike traditional risk models with static rule sets that can only search for known threats, AI-based tools and techniques can identify patterns and anomalies at a much more granular level, and quickly adapt and respond to evolving operating conditions and threats over time. One recent study, for example, demonstrated how the use of AI can improve real-time anomaly detection in high-value payments systems (HVPSs), many of which still rely on traditional rules-based and ad-hoc monitoring approaches; the proposed ML framework was used to successfully overcome a key challenge in HVPSs of identifying anomalies in large, complex datasets, where pre-identified examples of anomalous transactions – which are typically important for training anomaly detection systems – are rare.[7]

## Response

Resolving operational incidents often involves time-consuming manual investigation and decision-making processes. This is a particular issue for entities being affected by an incident at another PSP, in which case the information available to inform timely incident analysis and response may be particularly limited. In the case of both operational outages and cybersecurity attacks, AI could be used to automate incident investigation and provide clear summaries of the relevant information to humans, enabling much faster response times. Deep learning tools could help analyse and understand any detected malware, and potentially even reverse-engineer an attack. AI systems could also automatically apply appropriate countermeasures in response to certain attacks in real time, reducing the need for human involvement and significantly increasing the speed of response. For example, if an AI system identifies anomalous

[7] Desai, Kosse & Sharples (2024), Finding a needle in a haystack: A machine learning framework for anomaly detection in payment systems, BIS Working Papers, No. 1188, May.

behaviour in a particular part of the network that may be indicative of an attack, it could automatically block and quarantine those network endpoints.

An important example use case for AI in payments is application programming interface (API) security. APIs have become increasingly important for interlinking entities across the payments ecosystem. While access control is a key aspect of API security, it is also a common threat domain that can expose large amounts of data and functionality through both simple misconfigurations and complex attack vectors. AI can be used to enhance API access control not only by detecting vulnerabilities or anomalous behaviour in real time, but also automatically adopting risk-based responses to any potential issues; such responses could include refusing access, stepping up authentication requirements, or even revoking or limiting access of authorised users exhibiting unusual behaviour (in the case of potential attacks by internal actors).

If a network outage does occur, AI could help reduce the impact on customers and businesses through enhanced transaction authorisation decisioning. Currently, PSPs often rely on static rules-based models as a backup for managing payments in the event of an outage. This generally leads to a large number of declined transactions. The advanced use of AI can reduce this impact. Visa and Mastercard, for example, now offer AI-based stand-in processing services, which enable the card schemes to make increasingly accurate authorisation decisions on behalf of an issuer during a service disruption; these services rely on AI models that are trained on large cardholder activity data sets to predict how the issuer would have responded to each authorisation request in normal circumstances.

## OPPORTUNITY 3: OPERATIONAL EFFICIENCY

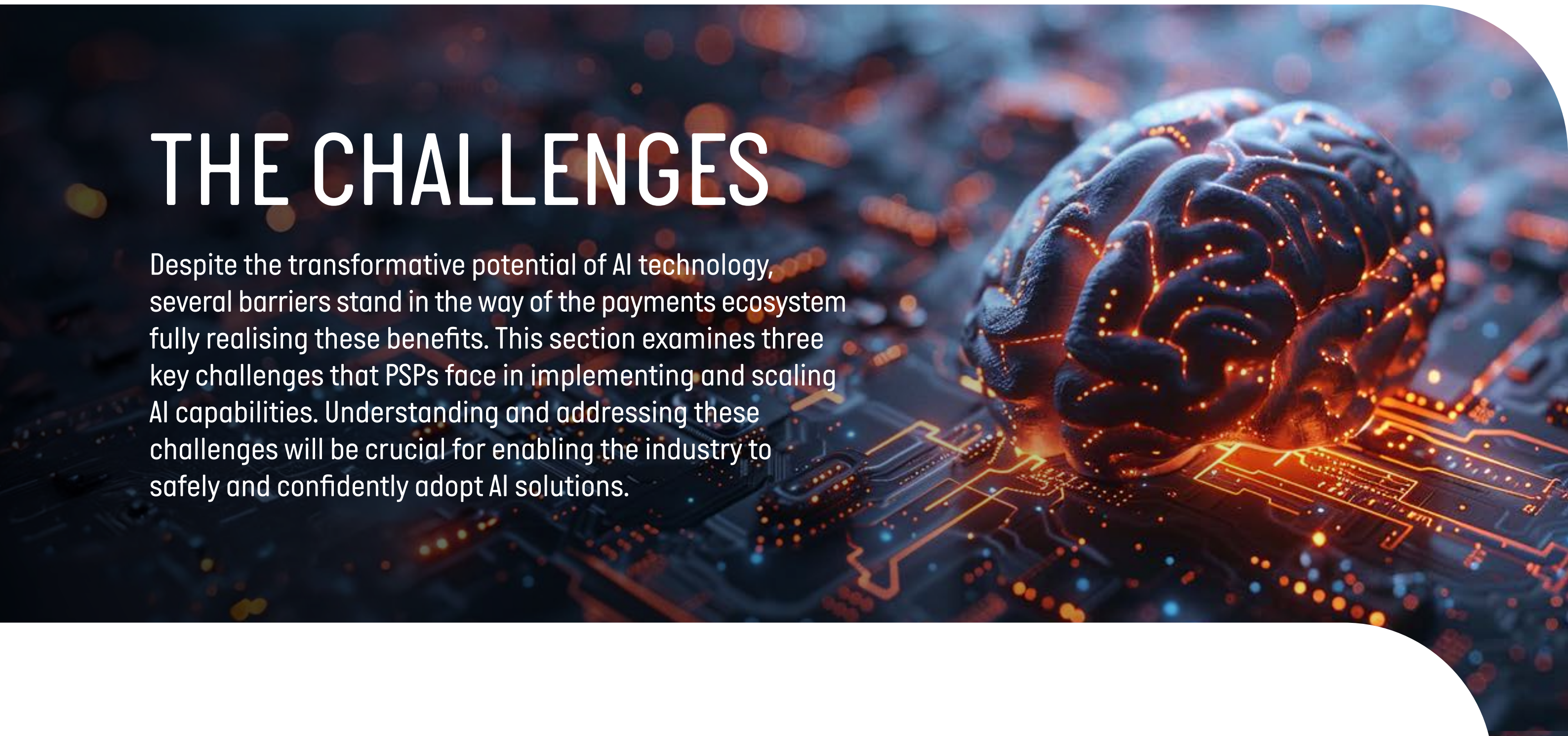
One of the most commonly cited benefits of AI for businesses is its potential to help improve operational efficiency. For PSPs, some of the key opportunities here include:

- streamlining operations and further automating manual tasks involved in payment reconciliation (including data entry, matching, and exceptions handling)
- automating the handling of payment-related customer inquiries and disputes
- automating compliance and regulatory reporting tasks
- increasing the speed and accuracy of payment processes.

Less frequently discussed is the potential for AI to drive operational efficiencies in organisational and industry transformation initiatives. A key issue faced by many incumbent PSPs is legacy infrastructure, which can pose challenges for innovation, efficiency and resilience. Some financial institutions have already begun to test the use of GenAI-enabled 'copilots' to automate certain developer tasks and assist software engineers by helping write new code, design software architecture, carry out testing, and recommend improvements to existing code. Such capabilities could be further leveraged to give AI an important role in streamlining key processes and managing some of the risks involved in migrating away from legacy infrastructure. This could include:

- analysing the legacy applications and system components to help inform the migration strategy
- facilitating the migration of data to the new infrastructure through data discovery, mapping and transformation
- automating the provisioning and deployment of new systems and setting up configurations on the new infrastructure stack
- testing and validating the migrated applications and systems
- helping identify and mitigate migration risks through ongoing systems monitoring
- providing insights and recommendations to assist decision makers in planning and executing the migration strategy.

One of AusPayNet's key strategic pillars is leading industry transformation initiatives to drive efficiency and innovation. Many of these transformation projects involve a significant amount of work by a large number of industry participants, often spanning several years. As part of industry stakeholders' participation in these initiatives, they could usefully explore opportunities for using AI to increase the efficiency and reduce the risks associated with the projects, both at the individual participant level and collectively. During the recent industry migration to the ISO 20022 messaging standard, for example, AI tools could have assisted industry participants in automating the complex data mapping and transformation process, reducing manual effort and potential errors. AI could also have been employed to analyse and monitor the impact of the migration on existing systems and processes across institutions, helping to identify potential issues and streamline the transition.



# THE CHALLENGES

Despite the transformative potential of AI technology, several barriers stand in the way of the payments ecosystem fully realising these benefits. This section examines three key challenges that PSPs face in implementing and scaling AI capabilities. Understanding and addressing these challenges will be crucial for enabling the industry to safely and confidently adopt AI solutions.

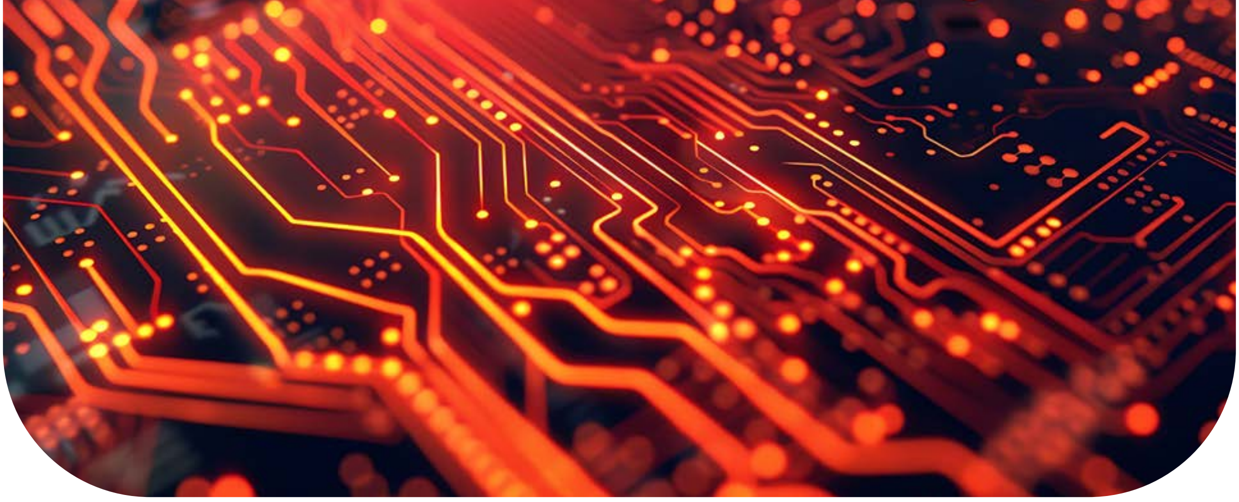
## CHALLENGE 1: IMPLEMENTATION AND DATA

While general-purpose AI tools are becoming increasingly accessible, effectively developing and integrating tailored AI models into a PSP's operations often requires considerable effort. This includes setting up the data and technical infrastructure, developing and validating the model, integrating it into existing systems and processes, and establishing appropriate governance and ongoing risk management arrangements. Both the initial setup and the ongoing maintenance and oversight of AI systems also require significant investments in talent and resources, creating high barriers to implementation. This is exacerbated by the persistent skills gap in the AI and data science domains in Australia.

One of the biggest implementation challenges for financial institutions revolves around data. The effectiveness and reliability of an AI system depends critically on the quantity and quality of data available to it. Issues such as inaccuracies and bias in the input data could have a substantial impact on the model outcomes, which in turn could have detrimental effects on users and the broader payments system.

In terms of quantity, the marked shift to digital payment methods – and digital services more broadly – over the past decade means that PSPs have substantially more customer and operational data than ever before. However, the quality, accessibility and usability of this data have not always kept pace. Several key challenges therefore arise that may constrain the development of trustworthy AI models in the payments ecosystem:

- **Data quality and usability:** AI models rely on high-quality data for training and implementation. In the payments industry, however, legacy data can often be inconsistent, incomplete, or unstructured. While the industry's migration to the ISO 20022 messaging standard should help address some of these challenges going forward, the enduring issues with historical data may limit its usability.
- **Data availability:** For many larger financial institutions, customer data is often siloed across systems or departments, posing challenges in accessing and integrating the necessary data sets into AI models. Some entities also have short transaction data retention periods, reducing the quantity of information available for model training.
- **Data fragmentation:** Relatedly, the emergence of newer players in the industry, and the rising number of customers using multiple financial institutions, means that customer data is becoming increasingly fragmented. Seeing only a portion of each customer's activity makes it more difficult for a PSP to build up individual customer profiles for enhanced personalisation, fraud monitoring and risk assessment. This issue also arises in the fragmentation of operational data across organisations – particularly in the case of distributed payment networks – which could make it difficult to realise AI-driven operational resilience benefits at a system level.
- **Data privacy:** Privacy and security regulations are a critical consideration for any data use and data sharing arrangements, both within organisations and across the industry. Some forms of collaborative analytics, for example, may not meet



existing privacy law requirements due to the sensitive nature of customer data that would need to be shared.[8]

- **Data interoperability:** Even where data sharing across institutions is possible, issues arising from differences in data formats and standards (present even within organisations) would be amplified at the industry level. While the move to ISO 20022 should greatly improve data interoperability in the payments ecosystem going forward, integrating historical and non-payments data from multiple organisations would likely require substantial standardisation work.

While AI itself could help overcome some of these issues (such as digitising documents and transforming data), others may face regulatory hurdles or require significant resource investment. Strong data management practices will therefore be critical for all PSPs deploying AI technology. Entities will need to assess and understand their data, and then work to address any identified limitations and implement appropriate data controls and infrastructure. This should include establishing data governance frameworks that seek to ensure the quality – including completeness, consistency and accuracy – of the data, and the robustness of systems and processes used to collect, store and manage the data.

## CHALLENGE 2: GOVERNANCE FRAMEWORKS

Putting in place robust AI governance frameworks is critical for organisations to effectively manage the risks associated with the development and deployment of AI systems. These frameworks should establish clear guidelines, processes and mechanisms for addressing matters such as accountability, transparency and explainability, fairness, safety, data privacy and security, and regulatory compliance. Implementing new AI capabilities without the proper governance and risk management frameworks is likely to lead to performance and operational issues, with the potential for significant user harm and loss of trust.

Considerable work is being undertaken by both the private and public sectors globally to establish governance frameworks to guide the development and implementation of safe and trustworthy AI. These now include the UNESCO *Recommendation on the Ethics of AI*, the OECD *AI Principles*, and the National Institute for Standards and Technology (NIST) *AI Risk Management Framework*. In Australia, the Government has developed an *AI Ethics Framework* and a *Voluntary AI Safety Standard*, which provide guidance to Australian businesses on how to safely and responsibly use and innovate with AI.

Notwithstanding this work, the unprecedented pace of development in AI technology over the past few years has left many organisations without the necessary knowledge, expertise and tools to safely and confidently deploy AI in line with the emerging safety standards. The *Australian Responsible AI Index* illustrates this gap, showing that only 29 per cent of organisations across the economy have demonstrably implemented practices in line with the *AI Ethics Principles*.[9] Assuming a similar gap exists in the payments ecosystem, entities' concerns about their ability to develop and deploy AI systems responsibly could hinder the industry's ability to realise the opportunities presented by AI.

The challenge of implementing effective governance frameworks in the payments industry manifests in several critical areas. One key example is model validation and oversight – as reliance on AI-based decision-making increases, PSPs will need robust capabilities to monitor model performance, identify any issues, and implement corrections. This is especially challenging in contexts such as anti-money laundering and counter-terrorism financing

[8] The Australian Government is currently reviewing both the *Privacy Act 1988* and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. The review of the latter is expected to include amendments to the tipping-off offence, which should enable improved collaboration between financial crime teams across the ecosystem.

[9] Fifth Quadrant (2024), *Australian Responsible AI Index 2024*, 5 September.

```
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the
```

(AML/CTF) operations, where the extended timeframes of investigations into suspected criminal activity (often spanning several years) complicate the validation of model effectiveness.

Moreover, the inherent complexity of advanced AI systems – often described as 'black box' models – creates additional governance challenges around risk management, transparency, and explainability. While new tools and techniques are emerging to address these challenges, many organisations lack the specialised expertise needed to effectively implement and use these solutions. This expertise gap becomes particularly critical as AI systems are granted greater autonomy in decision-making processes, requiring more sophisticated governance mechanisms to ensure safety and reliability.

## CHALLENGE 3: REGULATORY UNCERTAINTY

Rapid developments in AI capabilities over the past few years have prompted governments and regulators worldwide to reassess how these technologies should be regulated and supervised. Alongside many of our peer jurisdictions, the Australian Government is actively developing a regulatory framework for safe and responsible AI. In September, the Government launched a consultation on mandatory guardrails for the development and deployment of AI in high-risk settings.[10] The proposed guardrails aim to mitigate potential harms from AI by requiring developers and deployers of the technology to implement preventative measures around testing, transparency and accountability. The consultation paper noted that while "*ethics principles can help improve safe and responsible practices within organisations developing and using AI… effective regulation and enforcement is also needed, to create the right settings for AI innovation and adoption.*"

At this stage, however, the regulatory settings remain far from settled, both domestically and internationally. This uncertainty extends beyond the proposed regulation of AI in high-risk settings to encompass how existing laws, standards and regulatory frameworks will evolve to address AI-specific challenges. PSPs must navigate this ambiguity across multiple regulatory domains, including privacy, consumer protection, anti-discrimination, competition, data protection, and copyright laws – many of which may require amendments or additional guidance to effectively govern AI applications.

As acknowledged in the recent consultation paper, the current lack of regulatory clarity and certainty could be presenting barriers to AI adoption, and impeding businesses' ability to realise the full potential of the technology. In the payments industry, for example, PSPs may delay deploying more sophisticated fraud detection models or hesitate to increase their reliance on automated decisioning for real-time payments, due to uncertainty around future regulatory requirements for model transparency and explainability. There is also significant uncertainty around whether the ongoing reviews of AML/CTF and privacy laws will remove the legal barriers to the information sharing required to develop collaborative analytics tools for industry-level (and cross-industry) detection and prevention of economic crime.

AusPayNet therefore welcomes the Government's prioritisation of delivering regulatory clarity and certainty on this topic, and ensuring that Australia has a fit-for-purpose regulatory regime that will address the risks of AI while promoting continued innovation and adoption. We encourage financial services regulators to similarly prioritise the development of clear guidance on their approach to supervising the use of AI within the industry. Such clarity will provide organisations with the confidence needed to proceed with strategic investments in these capabilities. As the self-regulatory body for the payments industry, AusPayNet stands ready to assist in developing any technical standards or guidelines that may be required to ensure consistent application of AI safety principles across the payments ecosystem.

[10] Australian Government (2024), *Introducing mandatory guardrails for AI in high-risk settings: Proposals paper*, 5 September.

# THE RECOMMENDATIONS

While individual PSPs can take steps to address the challenges discussed above, many of the barriers to AI adoption in the payments ecosystem could be more effectively overcome through industry collaboration. This section proposes a set of practical recommendations for how industry participants can work together to overcome the highlighted challenges, and create an environment that enables the safe and responsible adoption of AI capabilities for the benefit of all ecosystem participants and end users.

## RECOMMENDATION 1: PRIVACY-ENHANCING TECHNOLOGIES

Given the potential benefits of AI-enabled collaborative analytics in the fight against economic crime, AusPayNet recommends setting up an industry working group to assess the feasibility of establishing such capabilities at an ecosystem level using privacy-enhancing technologies (PETs).

PETs enable the shared collection, processing and analysis of information while preserving the confidentiality of sensitive data. One PET method of note is Federated Learning, a framework that enables the collaborative training of a 'global' ML model across multiple decentralised data sets. In traditional ML systems, data is gathered from different sources and brought to a central location for training the model. With Federated Learning, the model is taken to the data instead. A central server initialises and distributes the preliminary model parameters to participating data holding entities. The model is then trained locally on each entity's database, computing siloed updates to the model parameters based on that data. The model updates from each entity (not the raw data) are then sent back to a centralised server, which aggregates them into an improved global model. The updated consensus is then redistributed across entities for the next round of training. This cycle continues iteratively until the global model converges or reaches the desired performance.

Such an approach could be incredibly powerful for strengthening industry-wide defences against economic crime. The decentralised training approach would ensure that the privacy and security of confidential customer information is preserved, while allowing all participants to benefit from the combined knowledge of the industry. As the iterative learning process continues over time and the AI algorithm adapts to emerging threat patterns and changes in customer behaviour, this intelligence would be shared across all participants through automatic model updates, ensuring that the information can be acted upon in a timely manner. This should enable more accurate identification of risks across the industry, including complex criminal activity spanning multiple PSPs. Such models could also be extended to enable cross-sector and cross-border collaboration.

Several global organisations, including the Financial Action Task Force, have already highlighted the potential of PETs for enabling more effective detection of economic crime across payments ecosystems, while overcoming many legal and operational challenges. Some organisations have already begun experimenting. The Bank for International Settlements (BIS), for example, recently conducted a proof-of-concept that found that collaborative analysis and learning arrangements were more effective in detecting money laundering networks than the current siloed approach, in which financial institutions carry out analysis in isolation.[11] The UK-US PETs Prize Challenges in 2022 called on innovators to develop Federated Learning solutions to help tackle the international money laundering problem, building on the work of a Tech Sprint held by the UK Financial Conduct Authority in 2019. SWIFT also recently launched a collaboration with Microsoft to build an anomaly detection model for transactional data across its global member banks using Federated Learning techniques.

Of course, the implementation of PETs is not without its own risks and challenges. Many of these are similar to the general challenges of implementing

[11] BIS (2023), Project Aurora: the power of data, technology and collaboration to combat money laundering across institutions and borders, 31 May.

AI-based tools, including issues related to data quality and interoperability, technical implementation, governance, and model risk management. Additional considerations in the case of collaborative analytics include differing risk appetites, commercial interests and investment priorities among participants. An industry working group should consider the practical feasibility of setting up such collaborative analytics capabilities for the Australian payments system, and develop a proposal for establishing an equitable arrangement that would encourage broad participation from across the ecosystem.

## RECOMMENDATION 2: INDUSTRY TELEMETRY ANALYTICS

Given the significant disruptions that could be caused by operational outages and cyberattacks in the payments ecosystem, AusPayNet encourages Members to continue pursuing enhancements in their own operational resilience, including through the opportunities discussed above. However, we also recommend that an expert industry working group be set up to carry out a feasibility study on developing a system-wide, AI-enabled telemetry analytics capability for relevant payments systems.

In the same way that AI could assist individual PSPs in preventing, detecting and responding to operational issues, the same opportunities could be realised at a system level. This is becoming particularly important as the number of entities – and interdependencies – in the payments value chain increases. As with economic crime, having access to operational information across the payments value chain could help participants more effectively identify and respond to vulnerabilities and threats than would be possible on a siloed basis. A centralised, system-wide telemetry capability could provide such visibility and information-sharing arrangements for participants. AI-enabled analytics embedded within this could then be used to help detect and respond to issues as they arise in real-time, with the potential to enable centralised decision making.

As with PETs, establishing such capabilities would not be without its own challenges. We therefore encourage a technical working group to conduct a similar feasibility study for such an initiative, exploring the issues and considerations highlighted in the first recommendation above.

## RECOMMENDATION 3: KNOWLEDGE SHARING

The rapid developments in AI technology over the past few years – and the corresponding need to urgently understand and address the potential risks it could present – have prompted a number of collaboration and information-sharing forums to be set up around the world.

AusPayNet similarly believes that appropriate industry knowledge sharing on matters related to the safe and effective deployment of AI in payments could benefit all ecosystem participants, including by enabling the collective development of solutions to common challenges. We therefore recommend setting up a dedicated industry advisory group focused specifically on AI in the Australian payments ecosystem, to help PSPs safely accelerate innovation and adoption of AI tools in the local industry context. Such an advisory group could share lessons learned, best practices, and insights into topics such as:

- regulatory compliance and the application of laws and standards to payments-specific AI use cases
- strategies for bias detection and mitigation in payments-related AI models
- approaches to enhance AI model transparency and explainability for more informed decision-making
- techniques for integrating AI with existing payment infrastructure and legacy systems
- effective frameworks for AI model risk management, monitoring, and validation
- emerging use cases and developments in AI capabilities that could address common industry issues and challenges
- cybersecurity best practices.

By fostering a culture of collective learning and knowledge sharing, the payments industry can navigate the complexities of AI adoption more effectively, reduce duplicative efforts, build trust with regulators and end users, and realise the full potential of developments in AI capabilities for the benefit of the ecosystem.

As part of this work, the industry should take a proactive stance on the adoption of AI governance and risk management frameworks, informed by the domestic and international efforts already underway in this space. This would provide a strong basis for further collaboration with the relevant regulators on shaping any future regulatory obligations that may apply in the context of the opportunities discussed above. If the industry deems it helpful, AusPayNet could also facilitate the development of guidance or technical standards for the application of AI in specific use cases.

# CONCLUSION

The continued advancements in AI capabilities present transformative opportunities for enhancing the safety, efficiency and resilience of the Australian payments ecosystem. From strengthening defences against increasingly sophisticated economic crime to improving operational resilience and efficiency, AI has the potential to address many of the industry's longstanding challenges. However, realising these benefits will require overcoming a number of implementation barriers related to data, governance frameworks, and evolving regulatory requirements.

While individual organisations can take steps to address these challenges, industry collaboration will be crucial for fully capturing the opportunities presented by AI technology. The recommendations proposed in this paper – exploring PETs for collaborative analytics, developing system-wide telemetry capabilities, and establishing knowledge-sharing arrangements – provide practical pathways for the industry to work together in overcoming some of the barriers to the adoption of enhanced AI capabilities. AusPayNet's Emerging Technology Experts Group will explore these recommendations in further detail over the coming months, with the aim of helping create an environment that enables the safe and responsible adoption of AI capabilities for the benefit of all ecosystem participants.

# GLOSSARY

**Artificial Intelligence (AI)**

Computer systems capable of performing tasks that typically require human intelligence, such as learning, reasoning, and making decisions, without explicit human instruction. AI encompasses various specialised domains that focus on different tasks, including Machine Learning (ML) (which enables computers to learn from data), Computer Vision (allowing them to interpret visual information), and Natural Language Processing (for understanding and generating human language).

**Deep Learning**

An advanced form of ML that uses artificial neural networks to learn and understand complex patterns in data, especially in tasks like visual recognition and speech synthesis, enabling more sophisticated analysis and decision-making capabilities than traditional ML approaches.

**Federated Learning**

A distributed ML approach that enables multiple parties to collaboratively train AI models without sharing the raw data, preserving data privacy and security.

**Generative AI (GenAI)**

AI systems capable of creating new content – such as text, images, audio, video, and code – by learning patterns from existing data.

**Machine Learning (ML)**

A subset of AI that allows computer systems to autonomously learn and improve their performance on a specific task through experience, without being explicitly programmed.

**Neural Networks**

Computing systems inspired by the human brain’s structure, consisting of interconnected nodes or ‘neurons’ that work together to analyse and learn from input data.

**Privacy-Enhancing Technologies (PETs)**

Technical methods that enable the processing and analysis of data while protecting the privacy and confidentiality of the underlying information.

**Telemetry Analytics**

The process of collecting, monitoring, and analysing data from distributed systems to detect patterns, anomalies, and potential issues across a network.