MASTERCARD CLICK TO PAY

Sydney International Business Competition
Case Two

SIBC 2025
SYDNEY INTERNATIONAL BUSINESS COMPETITION

SCC
SYDNEY CONSULTING CLUB

THE UNIVERSITY OF SYDNEY
Business School

Acknowledgements

CASE WRITERS

Wilson Thai
Jibreel Baytieh

BRIEF DESIGN

Wilson Thai
Jibreel Baytieh

OVERSEEN BY

Wes Hamilton-Jessop

SPECIAL THANKS TO

On behalf of SIBC 2025, the case writers would like to thank the following people for their invaluable input throughout the case writing process:

Mastercard Team
Min-Sik Son
William Zhang
Matthew Lee
Parth Patel
Faith Wong

In collaboration with the University of Sydney Business School. The Business Ethics Collaborative within the University of Sydney Business Chapter of Beta Gamma Sigma is proud to support student initiatives for the greater good of society.

Last edited: July 2025

MIN-SIK SON | WILLIAM ZHANG

Letter from Mastercard

Click to Pay: Securing the Future of Digital Commerce

Dear Teams,

We're thrilled to welcome you to the 2025 Sydney International Business Competition and proud to partner with Sydney Consulting Club for this exciting challenge.

At Mastercard, our mission is to connect and power an inclusive digital economy that benefits everyone, everywhere – and at the heart of that is making commerce simpler, safer, and smarter. One of our key innovations in this space is Click to Pay, a fast, secure, and password-free checkout experience designed to streamline online shopping for consumers and merchants alike.

This year's case invites you to step into our shoes and think critically about how Mastercard can elevate the Click to Pay experience – driving broader adoption, improving customer engagement, and unlocking value for merchants in an increasingly competitive digital landscape.

As future business leaders, we encourage you to approach this challenge with creativity and commercial insight. Consider not just the technology, but also the behavioural shifts, partnership opportunities, and strategic levers that can make frictionless checkout a preferred experience for all. We're excited to see the bold ideas and diverse perspectives you bring. On behalf of the Mastercard team, thank you for your participation, and best of luck in the competition!

Warm regards,

Matthew Lee
Head of Strategy

Table of Contents

Introduction to Mastercard **1**
2030 Vision: A World Without Card Numbers 2
The Changing Payments Landscape **3**
Cardless Commerce, Friction, and Fraud 3
Mastercard's Response: Click to Pay 3
Payments Technology 101 **5**
Card-Not-Present Payments 5
Tokenisation vs. Encryption 5
Payment Interoperability 5
Beyond Cards: Mastercard's Value-Add Services **7**
Cybersecurity and Fraud Prevention 7
Loyalty, Marketing, and Engagement Services 7
Data Intelligence and AI-Powered Analytics 7
Digital Identity and Secure Authentication 8
Financial Inclusion and Social Impact 8
Stakeholder Landscape **9**
Stakeholder Deep Dive: Consumers 9
Stakeholder Deep Dive: Merchants 10
Stakeholder Deep Dive: Banks and Card Issuers 11
Competitive Landscape **13**
Apple 13
Visa 14
Paypal 15
American Express 15
Your Challenge **17**

Table of Contents

Appendices **18**

Appendix A: Comparison of Click to Pay versus Contactless Cards 18

Appendix B: Payments Fraud Types Overview 19

Appendix C: Credit Card Fraud Statistics 21

Appendix D: The Role of Generative AI in Addressing Fraud 22

Appendix E: Payments Purchasing Processes 23

Appendix F: Mastercard Tokenisation Infographic 24

Appendix G: Consumer Trends 25

Appendix H: Merchant and Issuer Trends 27

Appendix I: Embedded Payment Ecosystems 29

Appendix J: Competitive Landscape Table 30

Introduction to Mastercard

Mastercard is a global technology company at the forefront of the payments industry. With operations spanning more than 210 countries and territories, Mastercard facilitates billions of secure transactions every year across physical, digital, and increasingly tokenised environments. Its core mission is to build a more inclusive and connected digital economy – one where individuals, financial institutions, businesses, and governments can interact with confidence, regardless of device, geography, or scale.

While best known for its branded debit, credit, and prepaid cards, Mastercard's role in the financial ecosystem extends far beyond card issuance. It serves as a foundational infrastructure provider, ecosystem coordinator, and innovation partner across the entire commerce value chain. Its reliable, scalable, and interoperable network enables commerce across every major payment channel: in-store point-of-sale (POS), e-commerce, in-app, peer-to-peer (P2P), and business-to-business (B2B).

Mastercard engages with a wide range of stakeholders and facilitates secure, real-time connectivity among them. These include:

Consumers – At the centre of every transaction is the end user. Mastercard serves over 3 billion cardholders globally, providing them with seamless access to their funds and enabling purchases across all digital and physical channels. Consumers benefit from Mastercard's multi-layered security protocols, its commitment to privacy, and innovations like contactless payments, mobile wallets (e.g., Google Pay, Samsung Pay), and tokenised checkout options. Mastercard's Priceless campaign and consumer rewards programs also help build brand trust and engagement across markets.

Merchants – Retailers, service providers, and online marketplaces rely on Mastercard to deliver fast, secure, and consumer-friendly payment experiences. From small businesses using QR code acceptance via Mastercard's Tap on Phone product to large enterprises integrating advanced tokenisation, merchants benefit from Mastercard's extensive suite of payment and security innovations. Mastercard's partnerships span every major retail sector – from physical stores such as Woolworths and Best Buy to digital-first platforms like Netflix, Uber, and Shopify.

Issuers – Mastercard works with thousands of banks and fintech institutions globally to issue Mastercard-branded payment credentials, including debit cards, credit cards, prepaid cards, and digital wallets. These credentials grant consumers and businesses access to funds and credit, enabling frictionless payments domestically and cross-border. For example, a Mastercard debit card issued by a regional bank in Kenya can be used for digital purchases from global e-commerce platforms such as Amazon or Alibaba. Additionally, Mastercard partners with global and regional acquirers – including Adyen, Stripe, Fiserv, and Worldline – to enable merchant acceptance across online and offline channels. Through these relationships, Mastercard provides tools for fraud prevention, dispute resolution, and security, supporting a resilient and efficient acquiring ecosystem.

Unlike some competitors that rely on proprietary platforms or closed ecosystems, Mastercard's philosophy is grounded in interoperability and openness. Its payment infrastructure and product offerings are designed to work across devices, operating systems, browsers, and financial institutions. Whether a consumer uses an iPhone, Android device, desktop browser, or smartwatch, Mastercard's solutions are built to enable consistent, secure, and seamless payment experiences.

This open-architecture model allows Mastercard to integrate with a broad range of ecosystem players, both legacy and emerging. For instance, Mastercard's APIs support integration with digital wallets, crypto platforms, embedded finance providers, and BNPL (buy now, pay later) firms.

Mastercard is also deeply invested in sustainability, financial inclusion, and ethical technology. It has pledged to bring 1 billion people and 50 million micro and small businesses into the digital economy by 2025. The Mastercard Centre for Inclusive Growth serves as a think tank and philanthropic arm that supports inclusive, sustainable economic development around the world.

Furthermore, Mastercard is a signatory to key ESG and carbon neutrality frameworks, and its product innovations including carbon tracking features integrated with banking apps, reflect its commitment to responsible commerce. The company is also actively engaging in public-private partnerships to strengthen cybersecurity, improve digital identity frameworks, and align digital payment systems with national financial goals.

2030 Vision: A World Without Card Numbers

Mastercard envisions a future in which digital payments are seamless, secure, and entirely numberless. As part of its strategic outlook for 2030, Mastercard has committed to eliminating manual card entry and removing visible card numbers from the consumer experience – both online and on physical cards. This transformation will be enabled through the widespread adoption of tokenised, biometric-first payment systems built with security embedded by design.

This vision extends beyond simply reducing fraud. It represents a fundamental reimagining of how trust is established in digital commerce. Rather than relying on vulnerable static credentials – such as card numbers, passwords, or CVVs – Mastercard aims to embed identity and authentication invisibly at every point of sale, thereby enhancing both usability and resilience.

By 2030, Mastercard has set forth the following objectives:

- Establish tokenisation as the default mechanism for all Mastercard transactions.
- Eliminate visible card numbers across all Mastercard-issued physical and digital cards.
- Deliver a frictionless checkout experience that functions securely across all devices, browsers, and platforms.

This vision reflects Mastercard's broader commitment to enhancing digital trust without sacrificing convenience. By embedding intelligence, interoperability, and advanced security directly into the payment infrastructure, Mastercard intends to make secure-by-default commerce the global standard.

The Changing Payments Landscape

Cardless Commerce, Friction, and Fraud

The global commerce landscape is undergoing a profound shift. As physical payment cards gradually disappear from wallets and point-of-sale terminals, digital and card-not-present (CNP) transactions are fast becoming the dominant mode of consumer payments. However, this evolution – while improving convenience – has also introduced significant vulnerabilities.

CNP environments, which include online and in-app transactions, have emerged as a focal point for payment fraud. In Australia alone, more than AUD 1 billion is lost annually to CNP fraud, with this figure trending upward year-on-year. These losses are driven by the inherent weaknesses of current checkout systems, which depend on the repeated entry, transmission, and storage of sensitive card credentials.

Industry data reveals that as much as 70% of all online payment fraud occurs during the digital checkout phase. Malicious actors exploit fragmented security measures, compromised endpoints, and inconsistent authentication protocols. This results in a growing erosion of consumer confidence, particularly in markets or demographics where digital literacy remains limited.

Mastercard's Response: Click to Pay

Click to Pay offers a transformative value proposition to each stakeholder in the payments ecosystem – consumers, merchants, and issuers – by addressing their core pain points while improving the overall efficiency, security, and user experience of digital commerce.

Click to Pay eliminates the need to manually enter card numbers, passwords, or shipping details when making purchases online. Instead, consumers can check out quickly and securely using a stored, tokenised version of their card credentials that are recognised across participating merchants and browsers. This leads to a faster, frictionless experience, particularly on mobile where typing sensitive information is cumbersome. Additionally, the use of tokenisation – combined with biometric or issuer-approved authentication – significantly reduces the risk of fraud. Consumers no longer need to trust individual websites with their card details, which improves peace of mind and reduces exposure to phishing, credential theft, and card-not-present fraud.

Click to Pay helps reduce cart abandonment by simplifying the checkout process. A shorter path to payment – without the need for account creation, login, or form-filling – improves conversion rates, particularly among mobile shoppers. The solution also supports device recognition and tokenised credentials, which protect against fraud while reducing the operational burden of PCI compliance. Merchants benefit from fewer chargebacks, lower fraud rates, and reduced checkout errors. Importantly, Click to Pay offers a consistent user experience across browsers and devices, enabling merchants to deliver seamless transactions without being locked into a specific platform, wallet, or hardware ecosystem.

Issuers gain a strategic opportunity to reassert their relevance in digital commerce. As more consumers rely on embedded or third-party wallets, issuers risk becoming invisible in the checkout experience. Click to Pay allows them to maintain brand visibility and control over transaction authentication while increasing approval rates through secure, tokenised transactions. It also reduces fraud liability by shifting sensitive data out of the payment flow and back into a secure, network-verified process. Moreover, the platform is built with issuer needs in mind – it supports scalable onboarding, token lifecycle management, and integration with loyalty programs, providing opportunities for personalisation and engagement that closed ecosystems often restrict.

In a major step forward, both the Commonwealth Bank of Australia (CBA) and Westpac have recently adopted Click to Pay on the issuer side, auto-enrolling millions of their cardholders into the service. This move significantly accelerates issuer-side readiness in the Australian market and shifts the strategic focus toward driving consumer awareness and merchant integration. With foundational adoption now in place, the next challenge lies in go-to-market execution across the broader ecosystem of consumers and merchants.

Payments Technology 101

Card-Not-Present Payments

In a typical card-not-present transaction – such as those occurring online or within mobile applications – a consumer manually enters their primary account number (PAN), expiry date, and CVV at checkout. This data is transmitted to the merchant's acquiring bank or payment gateway, which then routes the transaction through the card network (e.g., Mastercard) to the issuing bank. The issuer authorises or declines the transaction and relays the result back to the merchant in real time.

While this process appears seamless on the surface, it carries significant risks. Sensitive card credentials are frequently stored or transmitted in plain text, making them vulnerable to interception via phishing, data breaches, or malware. Additionally, because these credentials are static, they can be reused by fraudsters if compromised. Authentication procedures are inconsistently applied – ranging from SMS codes to nothing at all – leaving both consumers and merchants exposed to risk. Fundamentally, the system was engineered for physical cards, and as a result, it struggles to address the security and usability demands of the digital economy.

Tokenisation vs. Encryption

Tokenisation and encryption are both critical tools in the effort to secure digital data; however, they operate differently. Encryption protects information by scrambling it using a key, which can later be used to decrypt the original data. In contrast, tokenisation replaces sensitive data with a unique, non-sensitive placeholder, or "token," which holds no exploitable value outside its intended context. Unlike encryption, tokenisation cannot be reversed without access to a secure token vault.

In the context of payments, Mastercard employs network-level tokenisation. This approach ensures that real card numbers are never transmitted to merchants. Instead, Mastercard generates tokens that are uniquely tied to the specific merchant and device being used. These tokens are stored, authenticated, and processed in place of the actual card data, effectively neutralising the threat of data breaches. The token vault – maintained by Mastercard – governs these credentials and applies advanced authentication protocols, including biometrics and device analytics.

This differs from Apple Pay, which relies on device-based tokenisation. Apple stores tokens on a secure chip embedded in the device, enabling seamless in-app and contactless transactions – but only within Apple's ecosystem. While convenient for Apple users, this architecture is limited in scalability and interoperability, particularly for broader ecosystem integration across devices and platforms.

Payment Interoperability

EMVCo, a global consortium composed of Mastercard, Visa, American Express, Discover, JCB, and UnionPay, serves as the standards body for payment interoperability. Much like HTML enables consistency across web browsers, EMVCo develops the technical frameworks that allow payment systems to operate cohesively across devices, card brands, and geographies.

Click to Pay is built upon EMVCo's Secure Remote Commerce (SRC) standard. This standardisation enables merchants to integrate a single, universal interface that accepts tokenised payments from all participating networks. For consumers, this creates a predictable and trustworthy checkout experience, regardless of device, browser, or issuer. For banks, the SRC framework streamlines token issuance and provisioning at scale, ensuring consistent security practices across a diverse array of financial institutions. This commitment to open standards and cross-platform compatibility distinguishes Click to Pay from proprietary solutions that typically operate within closed environments.

In anticipation of global Click to Pay adoption, Mastercard has made substantial investments in the underlying infrastructure necessary to support a secure, tokenised ecosystem. The Mastercard Token Vault functions as a centralised, secure repository for issuing and managing tokens on behalf of issuers, merchants, and consumers. The Token Authentication Service (TAS) enables real-time verification of transactions by leveraging device signals, biometric inputs, and contextual heuristics.

To facilitate adoption by merchants, Mastercard provides software development kits (SDKs) and application programming interfaces (APIs) that simplify integration with existing e-commerce platforms. Additionally, all Mastercard tokenisation technologies are fully compliant with EMVCo standards, ensuring compatibility with other networks and seamless interoperability for merchants and issuers alike.

Beyond Cards: Mastercard's Value-Add Services

While Mastercard is globally recognised for its core role in facilitating card-based transactions, the company has, over the past decade, evolved into a multi-dimensional technology platform with a robust suite of value-added services. These expanded capabilities serve as powerful enablers for the success of Click to Pay, particularly in markets where security, personalisation, data intelligence, and trust infrastructure are prerequisites for adoption. Consultants developing go-to-market strategies must therefore not view Click to Pay in isolation, but as part of a broader Mastercard ecosystem – one that provides embedded solutions to common merchant, bank, and consumer frictions.

Cybersecurity and Fraud Prevention

Mastercard has made significant strides in fraud detection and prevention through its acquisition of cybersecurity firms such as RiskRecon and Ethoca. These platforms enable real-time threat intelligence, behavioural analytics, and anomaly detection across the payments ecosystem. Ethoca, in particular, facilitates merchant-issuer collaboration to resolve chargebacks before they occur, reducing fraud losses and operational costs. These tools not only build trust but also serve as key differentiators when merchants and issuers assess the risk profile of integrating new checkout technologies like Click to Pay. Mastercard's layered security architecture can be deployed as part of the onboarding journey to reduce barriers to adoption.

Loyalty, Marketing, and Engagement Services

Through Mastercard Advisors, the company offers advanced marketing and customer engagement tools that are deeply rooted in consumer spending behavior. This includes support for personalised loyalty programs, retargeting campaigns, and lifecycle engagement initiatives. These capabilities are particularly relevant for Click to Pay adoption campaigns, where Mastercard can enable merchants to offer personalised incentives (e.g., loyalty points or discounts) for first-time Click to Pay users. Additionally, Mastercard's capacity to segment audiences based on behavioral insights can inform high-precision outreach strategies that accelerate market penetration across geographies and industries.

Data Intelligence and AI-Powered Analytics

At the core of Mastercard's value proposition is its ability to convert billions of anonymised transactions into actionable insights. Leveraging advanced machine learning models and AI-driven platforms, Mastercard provides tools that help issuers and merchants identify high-value segments, understand conversion drop-offs, and optimise checkout flows. These tools can be integrated into Click to Pay rollout plans to continuously monitor performance, adjust strategies in real time, and A/B test incentive models. In addition, Mastercard's merchant analytics dashboards can help businesses assess the long-term value of Click to Pay adoption by quantifying impacts on cart abandonment, fraud reduction, and repeat purchases.

Digital Identity and Secure Authentication

Mastercard is actively building a global digital identity framework through its Mastercard ID service, which allows consumers to verify their identity across channels using biometrics, device signals, and verified credentials. This initiative is aligned with the company's broader vision of a password-free, token-based commerce ecosystem. For Click to Pay, this means the ability to offer seamless authentication experiences without reliance on static credentials like passwords or card numbers. Mastercard's investments in biometric partnerships and FIDO-based authentication protocols enhance the security layer behind Click to Pay, providing consumers with frictionless yet secure checkout interactions – especially critical in high-risk or high-value transactions.

Financial Inclusion and Social Impact

Mastercard's inclusive approach to payments is also reflected in its work with governments, non-profits, and development agencies. The company has introduced programs targeting financially underserved populations, including initiatives for smallholder farmers, displaced refugees, and unbanked women across Africa, Southeast Asia, and Latin America. These programs are powered by Mastercard's digital rails and often incorporate features such as microloans, mobile wallets, and identity verification services. As Click to Pay expands into emerging markets, these inclusion-focused initiatives can serve as deployment platforms – offering both infrastructure and community trust as entry points for digital commerce.

Stakeholder Landscape

The success of Mastercard Click to Pay depends on the coordinated activation of three primary stakeholder groups: consumers, merchants, and banks (card issuers). While each party plays a distinct role within the digital payments ecosystem, the full value of Click to Pay can only be realised through concurrent adoption across all three segments. This interdependency presents both strategic opportunities and significant go-to-market complexity.

Stakeholder Deep Dive: Consumers

Consumers represent a foundational pillar of the digital payments ecosystem. Consumers engage directly with the transaction interface – making real-time decisions about whether to complete a payment, trust the digital environment, or abandon the purchase altogether. These decisions are not guided solely by functional efficiency, but are shaped by a broader desire for trust, security, and convenience. Accordingly, the design and performance of the digital checkout experience exert a significant influence on both transaction completion and long-term brand loyalty.

Despite ongoing technological advancements in digital commerce, the consumer experience during online checkout – particularly in card-not-present (CNP) environments – remains fragmented and often inadequate. Online retail platforms, mobile applications, and subscription-based services frequently require consumers to manually enter sensitive card credentials. This process is increasingly viewed as both inconvenient and insecure. In Australia alone, losses attributed to CNP fraud exceed $1 billion annually, mirroring a global pattern in which over 70% of all payment fraud occurs online. These figures underscore a persistent misalignment between consumer expectations and the legacy systems that underpin digital transactions.

In this context, consumer concerns extend beyond functionality. The growing prevalence of phishing attacks, identity theft, and data breaches has heightened sensitivity to digital security risks – particularly when transactions occur over public networks or shared devices. As a result, consumers now demand payment experiences that are not only frictionless but also demonstrably safe. This shift in expectations creates a dual imperative for payment providers: to reduce complexity without compromising real or perceived trust.

Contemporary digital solutions must therefore recognise that trust and efficiency are no longer competing priorities, but simultaneous requirements. Understanding how these evolving consumer expectations manifest – and identifying the specific pain points within current checkout flows – will be essential to developing a go-to-market strategy that drives widespread adoption and sustained engagement.

The Need for Consistency Across Devices and Platforms

Consumer engagement with digital commerce frequently spans multiple devices and contexts. A single purchase journey may begin on a smartphone, continue on a desktop computer, and conclude within a mobile application. However, many existing digital wallets and payment interfaces are constrained by hardware or browser compatibility. For instance, solutions such as Apple Pay are limited to the iOS ecosystem and the Safari browser, thereby excluding consumers operating outside of that environment. Furthermore, user experiences are often inconsistent across different operating systems and browser types, which fragments the payment process and erodes user trust.

Expectations of Privacy, Control, and Data Stewardship

Modern consumers are increasingly conscious of how their personal and financial information is collected, stored, and used. High-profile data breaches and privacy scandals have elevated public awareness and skepticism regarding data handling practices. Although technologies such as tokenisation can provide robust protections by substituting sensitive card details with non-sensitive digital tokens, these measures often operate invisibly. A gap persists between the technical assurances embedded in modern payments infrastructure and the consumer's comprehension or appreciation of those safeguards. As a result, even secure systems can be perceived as untrustworthy if transparency and education are lacking.

Global Commerce and Subscription-Based Consumption

Digital commerce is increasingly transnational and subscription-driven. Consumers expect payment methods that can operate across jurisdictions, support recurring transactions, and seamlessly accommodate updates to payment credentials. These requirements are particularly relevant among younger demographics, such as Generation Z, who routinely maintain multiple active subscriptions for streaming, digital services, and e-commerce memberships. Consequently, digital payment systems must not only facilitate initial transactions but also sustain long-term payment continuity across platforms and geographies.

Stakeholder Deep Dive: Merchants

In today's increasingly competitive digital commerce environment, merchants face sustained pressure to deliver frictionless customer experiences while simultaneously safeguarding against escalating levels of online fraud. Among the most critical junctures in this environment is the checkout process – a pivotal moment at which consumer trust, brand credibility, and revenue outcomes are either strengthened or undermined. This challenge is especially acute in card-not-present (CNP) transactions, where purchases occur through websites or mobile applications, and the inherent risk of fraud is significantly heightened.

Merchants must carefully navigate the trade-off between streamlining the checkout process to minimise cart abandonment and maintaining stringent security protocols to prevent fraud, chargebacks, and data breaches. Many organisations, however, lack the specialised resources, technical infrastructure, or in-house expertise required to implement advanced solutions such as tokenisation, multi-factor authentication, or frictionless user experience enhancements. As a result, they are often more vulnerable to operational disruptions and reputational damage arising from security lapses or suboptimal customer journeys.

Ease of Integration

Many businesses lack deep technical expertise when it comes to implementing and managing secure payment systems. Without in-house payment specialists or development resources, they often depend on third-party platforms and out-of-the-box solutions to meet basic compliance requirements, such as PCI-DSS. As a result, the decision to adopt a solution like Click to Pay is typically driven by ease of integration rather than technical merit. If deployment involves complex development work, unclear documentation, or additional certification steps, adoption is likely to be deprioritised, particularly when the commercial benefits are not immediately evident.

Platform Fragmentation

Most merchants do not operate on a single technical stack. While some enterprises rely on in-house systems, the majority – especially SMEs – depend on third-party platforms such as Shopify, WooCommerce, or Adobe Commerce. Implementing Click to Pay across these environments requires not only technical compatibility, but also alignment with platform-specific workflows, plugin architecture, and front-end customisation constraints. For merchants using multiple storefronts or international domains, consistent implementation becomes even more complex. Many lack the in-house development resources to manage such integrations independently.

Cross-Border and Local Payment Integration

Merchants operating internationally must accommodate diverse local payment expectations – ranging from preferred authentication methods to regulatory requirements and acquirer capabilities. While Click to Pay offers a standardised checkout framework through tokenisation and consumer identity recognition, adoption can be hindered by uneven support across payment processors and markets. If local acquirers or platforms do not fully support the Click to Pay infrastructure, merchants may be forced to maintain multiple checkout systems in parallel, increasing operational complexity and reducing the consistency of the user experience. This fragmentation undermines the value proposition of a universal solution and may delay adoption by merchants with global footprints.

Stakeholder Deep Dive: Banks and Card Issuers

Banks and card issuers represent a foundational component of the global payments infrastructure, responsible for provisioning credit, debit, and prepaid instruments that facilitate secure consumer transactions across both physical and digital channels. The integrity and reliability of these institutions are closely associated with the safety and consistency of payments bearing their branding. However, in a rapidly digitising commerce landscape, issuers face intensifying pressure to uphold consumer trust, mitigate fraud, and maintain strategic relevance amid the rise of alternative payment solutions and increasingly intermediated checkout environments.

Limited Resources and Legacy Constraints

Many issuing banks, especially smaller or regionally focused institutions, operate under legacy core systems and constrained innovation budgets. Integration of new capabilities often competes with mandatory compliance projects such as open banking, ISO 20022 migration, or enhanced identity verification protocols. Click to Pay must therefore demonstrate low technical lift, minimal integration friction, and value that justifies investment – particularly when onboarding requires updates to customer-facing platforms, back-end fraud systems, or CRM workflows.

Brand Disintermediation

A potential long-term challenge confronting issuers is the risk of brand disintermediation. As consumers increasingly adopt embedded checkout experiences, one-click wallets, and Buy Now, Pay Later (BNPL) services, the issuer's role in the transaction is often rendered invisible. In many cases, the traditional payment card is neither presented nor acknowledged at the point of sale.

This development reduces issuers' ability to maintain top-of-wallet positioning, integrate loyalty schemes, or differentiate through personalised offers and experiences. Over time, this diminishes the issuer's strategic influence and relegates them to the status of a commoditised back-end processor – disconnected from the consumer relationship and vulnerable to displacement by more visible digital payment brands. Yet, Click to Pay offers a meaningful counter to this trend by preserving the four-party model. Unlike closed-loop or proprietary wallets (e.g. Xpays), Click to Pay ensures the issuer remains visible in the transaction, retains authentication control, and continues to shape the customer experience. This re-establishes the issuer's role in digital commerce and creates opportunities for loyalty integration, messaging, and brand continuity at the point of checkout.

Competitive Landscape

The competition to define and control the future of the digital checkout experience has intensified significantly over the past decade. Industry leaders have each adopted distinct approaches to addressing the same core challenge: how to enable online transactions that are both frictionless and secure. These approaches range from hardware-centric wallets and proprietary platforms to closed-loop payment systems and embedded browser solutions.

In this dynamic and increasingly fragmented landscape, Mastercard's Click to Pay positions itself not as another digital wallet, but as a universal, network-native protocol. Purpose-built for interoperability and aligned with EMVCo's Secure Remote Commerce (SRC) standards, Click to Pay represents a shift toward open, scalable, and device-agnostic payment infrastructure.

To design an effective go-to-market (GTM) strategy for Click to Pay, it is essential to analyse the strategic choices, product architectures, and deployment tactics of other major players in the digital payments space. Examining how companies such as Apple, PayPal, Visa, and American Express have entered and scaled in the market provides critical context for identifying competitive advantages, avoiding common pitfalls, and crafting a differentiated adoption plan tailored to Mastercard's ecosystem.

Apple

Since its launch in 2014, Apple Pay has established itself as a dominant force in the mobile and in-app payments landscape. Developed by Apple Inc., the platform exemplifies a vertically integrated payment solution – seamlessly combining proprietary hardware, software, and authentication technologies. This integration has allowed Apple to deliver a consistent and highly secure user experience, particularly within its own ecosystem of iPhones, iPads, Apple Watches, and Macs.

At the core of Apple Pay's security model is device-level tokenisation. When a user adds a card to Apple Wallet, the actual card number is never stored on the device or Apple servers. Instead, the system generates a unique Device Account Number (token), which is stored securely in the Secure Enclave – a dedicated security chip embedded in Apple devices. Each transaction is then authorised with a dynamic security code (cryptogram), and authenticated through biometric verification via Face ID or Touch ID. This end-to-end approach ensures that real card credentials are never exposed to merchants, transmitted during checkout, or visible to Apple itself.

Apple Pay's design prioritises both convenience and safety. In physical retail environments, it allows contactless tap-to-pay through near-field communication (NFC), while in-app purchases are streamlined with a single biometric confirmation. The result is a frictionless user journey with minimal cognitive load, particularly appealing to users already embedded in the Apple ecosystem.

However, this success comes with limitations. Apple Pay is exclusive to Apple hardware and compatible primarily with Safari as a browser, restricting its accessibility across non-Apple devices and limiting its influence in broader browser-based e-commerce.

The platform also functions as a closed-loop system, with Apple retaining significant control over interface design, payment routing, and data access. Merchants and issuers often have limited flexibility to customise the user experience, access token data, or integrate loyalty and marketing overlays.

In summary, Apple Pay has set the industry standard for secure, user-friendly payments within a closed ecosystem. Yet its effectiveness depends heavily on hardware ownership and platform loyalty, posing challenges for cross-platform interoperability and broad merchant adoption – especially outside of iOS environments.

Visa

Visa Secure is Visa's proprietary implementation of the EMV® 3-D Secure 2.0 protocol, designed to strengthen the security of digital transactions while preserving a seamless customer experience. It plays a critical role in mitigating the risks associated with online payments, particularly in card-not-present environments where fraud threats are more pronounced.

At the heart of Visa Secure is a dynamic, risk-based authentication (RBA) model. Rather than applying uniform security procedures to all transactions, the system intelligently evaluates each payment using over 100 data points in real time. These include device attributes, transaction patterns, geolocation data, and behavioural indicators. When a transaction is deemed low-risk, authentication occurs passively in the background, allowing the consumer to proceed without additional input. For transactions flagged as higher risk, Visa Secure escalates authentication using one-time passwords, biometric prompts, or other forms of step-up verification.

This adaptive approach achieves two objectives: it enhances fraud prevention while minimising unnecessary friction during checkout. By tailoring security measures to the risk profile of each transaction, Visa Secure contributes to higher approval rates, improved customer satisfaction, and reduced false declines – an outcome critical to both operational efficiency and end-user trust.

Furthermore, Visa Secure aligns with global regulatory mandates for strong customer authentication (SCA), including Europe's PSD2 requirements. Its architecture allows financial institutions to enforce rigorous authentication policies while maintaining a user-friendly interface, providing flexibility and compliance across jurisdictions.

By integrating advanced analytics and machine learning into the authentication process, Visa Secure represents a forward-looking response to the evolving landscape of digital commerce. Its ability to deliver targeted protection at scale positions it as a key component in building consumer confidence and safeguarding the integrity of online payments.

PayPal

PayPal is a widely recognised digital payments platform that enables individuals and businesses to send, receive, and manage money securely across online and mobile channels. As one of the earliest entrants into the digital wallet space, PayPal has evolved into a global fintech leader, serving over 400 million active users across more than 200 markets. Its widespread acceptance and consumer trust have made it a default option for many in both peer-to-peer transfers and e-commerce transactions.

Central to PayPal's offering is its ability to abstract sensitive payment information from merchants. When a user transacts through PayPal, their actual card or bank details are never shared with the merchant. Instead, PayPal acts as an intermediary, facilitating the transaction while protecting the underlying financial credentials. This model significantly reduces exposure to data breaches and offers a sense of privacy and control that appeals to risk-conscious consumers.

PayPal's ecosystem extends well beyond simple transactions. Its platform includes features such as buyer protection, dispute resolution, one-touch checkout, and seamless integration with digital marketplaces. These services collectively enhance user confidence and streamline the purchasing process, contributing to reduced cart abandonment and improved customer retention for merchants.

From a security standpoint, PayPal incorporates a multi-layered defence model that includes real-time risk monitoring, device intelligence, and AI-powered fraud detection. Users are also provided with two-factor authentication and biometric login options through the PayPal app, reinforcing account security while maintaining convenience.

PayPal's ability to operate across different funding sources – credit cards, debit cards, bank accounts, and PayPal balances – adds to its versatility. Furthermore, its merchant services include invoicing, subscriptions, pay-out management, and access to working capital, positioning it as a comprehensive solution for businesses seeking digital payment capabilities. As digital commerce continues to scale globally, PayPal remains a key player in the payment landscape, offering a mature, consumer-trusted platform with a broad suite of financial tools and services tailored to both end-users and enterprises.

American Express

American Express (Amex) has consistently differentiated itself from other global payment networks through its vertically integrated, direct-issuing model and its strategic focus on high-value clientele. This unique structure enables Amex to maintain end-to-end control over the cardholder experience – ranging from issuance and rewards to risk management and dispute resolution. Within this closed-loop framework, the company has developed Express Checkout, a proprietary digital payment solution designed to streamline online transactions for Amex cardholders.

Express Checkout enables authenticated Amex users to bypass the manual entry of card and shipping information by automatically populating these fields during online checkout. This capability is underpinned by Amex's internal data infrastructure, which facilitates real-time credential access while preserving data security. The solution is engineered to reduce checkout friction and accelerate transaction completion, particularly for repeat users within the Amex ecosystem.

A notable advantage of Express Checkout lies in its seamless integration with Amex's broader digital offerings, including its loyalty rewards programs, fraud protection mechanisms, and account management tools. This integration ensures that the benefits of card membership – such as reward accrual, promotional offers, and purchase protections – are preserved and consistently applied across the payment journey.

However, Express Checkout's strategic scope is intentionally narrow. It is exclusively available to users transacting with Amex-issued cards and is supported only by participating merchants who choose to integrate the feature. As such, its utility is largely confined to the Amex ecosystem. Unlike open-standard digital payment solutions designed for interoperability across networks and devices, Express Checkout does not seek to operate at scale beyond Amex's direct customer base.

Consequently, while Express Checkout reinforces American Express's brand positioning and enhances service delivery for existing customers, it does not function as a universal checkout solution. Its value lies in deepening cardholder engagement and loyalty rather than in expanding cross-network acceptance. Despite these limitations, the solution remains a competitive force in the premium segment of the digital payments market, particularly where personalised service, brand consistency, and secure convenience are prioritised.

Your Challenge

The future of secure, seamless online checkout remains fragmented. While interoperable, tokenised solutions like Mastercard Click to Pay offer clear benefits – reduced fraud, improved user experience, and a foundation for safer digital commerce – adoption remains uneven across markets and stakeholder groups.

Recent momentum in Australia signals a turning point. The Commonwealth Bank of Australia (CBA) and Westpac have both auto-enrolled millions of customers into Click to Pay, significantly accelerating issuer-side adoption. With key banks and issuers now onboard, the immediate challenge shifts to driving meaningful engagement among **consumers and merchants**, and building scalable go-to-market models that deliver results in the near term in Australia and possess the capability to be scaled globally. The challenge for your team is clear:

How can Mastercard drive meaningful growth of Click to Pay adoption in the Australian market over the next few years – while developing a go-to-market model that can scale globally?

There are several considerations that must be addressed to take the program as it currently stands towards this vision.

1. What are the most significant adoption barriers faced by consumers and merchants? What commercial, behavioural, or operational pain points are slowing uptake, and how should Mastercard prioritise these in its go-to-market efforts?

2. Given the evolving competitive landscape, how should Mastercard position and communicate Click to Pay's unique value proposition towards consumers and merchants? How can they distinguish Click to Pay from key competitors such as Apple Pay?

3. How can Mastercard execute an effective go-to-market strategy in Australia that addresses current adoption gaps while laying the groundwork for broader international expansion? How should the solution remain scalable and interoperable across ecosystems?

4. What role should Mastercard play in educating the market and shaping best practices? What value-add services, partnerships, or platform integrations might accelerate ecosystem activation?

Appendix A: Comparison of Click to Pay versus Contactless Cards

Click to Pay is Mastercard's solution to streamlining online payments in the same way contactless cards transformed in-store transactions. Both aim to eliminate friction at checkout by enabling fast, secure, and intuitive payment experiences.

Just as contactless cards allow consumers to tap and pay without PINs or signatures, Click to Pay allows users to check out online without manually entering card numbers, passwords, or shipping details. It relies on network-level tokenisation, device recognition, and biometric or issuer-approved authentication to reduce fraud and increase trust – particularly in card-not-present environments.

Importantly, both technologies embed security into the infrastructure itself, easing compliance burdens for merchants and reducing consumer anxiety around data breaches. Click to Pay also helps issuers maintain visibility during the digital transaction, preserving brand presence that is often lost in third-party wallets. By drawing on the behavioural success of contactless payments, Click to Pay offers a familiar, consistent, and scalable approach to online checkouts that benefits consumers, merchants, and issuers alike.

Feature	Contactless Cards (In-Store)	Click to Pay (Online)
Checkout Experience	Tap-and-go with no PIN for low-value amounts	One-click checkout without manual data entry
Security Mechanism	EMV chip + dynamic CVV	Tokenisation + device/biometric authentication
Fraud Risk	Low fraud rate due to embedded protections	Reduced CNP fraud through network-level tokenisation
User Effort	Physical tap, no PIN for most purchases	No login, password, or card entry required
Merchant Setup	NFC-enabled terminal	EMVCo SRC-compliant integration
Issuer Branding	Cardholder sees and uses bank-issued card	Issuer remains visible in the digital checkout flow
Consumer Trust Anchor	Physical card backed by trusted institution	Recognised Mastercard + issuer security infrastructure
Strategic Analogy	Behavioural normalisation of tap payments	Behavioural replication for digital checkouts

Source: https://www.mastercardservices.com/en/advisors/payments-consulting/insights/click-pay-e-commerce-counterpart-contactless-cards

Appendix B: Payments Fraud Types Overview

Account Takeover (ATO)
Criminals traditionally use techniques such as password sniffing, credential stuffing, or phishing to gain access to an account. Once inside, they quickly make unauthorized transactions or drain funds before the victim is even aware. The availability of GenAI, and malicious tools such as WormGPT and FraudGPT, allows criminals to easily scale phishing and malware attacks. More recently, fraudsters are stealing facial recognition data to bypass security checks and access bank accounts, as seen in recent campaigns by hackers in Southeast Asia. In addition to direct attacks, third-party ATO attacks are increasing, with data showing an 18% year-over-year increase in attacks in 2023, following a 52% year-over-year increase in 2022.

Transaction fraud
There are many shades of transaction fraud. One major concern is fraudsters' use of advanced methods to exploit stolen credit card data. These details, often acquired from breaches or fake merchant websites that harvest card credentials, result in costly chargebacks. Fraud often goes undetected until post-authorisation, leading merchants to ship goods that are later disputed, causing financial losses and unfilled orders.

Bank Identification Number (BIN) attacks
A particularly concerning type of transaction fraud is BIN attacks – where fraudsters use automated software to systematically test card numbers within a BIN to identify valid combinations. These attacks have surged by 80% globally since 2020.

Account onboarding and identity fraud
Fraudsters continue to exploit onboarding processes using stolen or fabricated identities to open bank accounts or pose as legitimate merchants. Synthetic identity fraud, which combines real and falsified information to create new identities, is particularly challenging to detect and is the fastest-growing financial crime in the U.S. GenAI and deep fakes exacerbate this threat by producing synthetic imagery and making fake identification documents difficult for fraud teams to detect during account onboarding and Know Your Customer checks. In some cases, fraudsters even spoof biometric data. To avoid detection, fraudsters often keep synthetic identity accounts dormant for months or years, securing good credit lines before committing bust-out fraud, where they max out credit and disappear without repayment.

Merchant fraud
Fraud by merchants is increasingly prevalent in the payments ecosystem as opening merchant accounts has become easier. Payment facilitators create thousands of new accounts daily, giving organized criminals opportunities to exploit the system and illegally open accounts for fraudulent activities. Fake merchant accounts can process purchases from stolen credit card information, defrauding issuers and leading to chargebacks. In some cases, individuals listed on anti-money laundering (AML) or anti-terrorist financing watchlists, or those originating from countries with economic sanctions, create merchant accounts using stolen or synthetic identities. Regulators expect acquirers to perform due diligence to prevent these activities, or face fines and reputational damage.

Source: https://content.ekata.com/Trusted-Transactions-The-common-good-Creating-an-ecosystem-of-transaction-trust.html

Appendix B: Payments Fraud Types Overview (Continued)

AML and regulatory compliance
Criminals exploit financial systems to launder money from illegal activities through placement, layering, and structuring. While financial institutions and other regulated businesses have systems to detect and prevent money laundering, traditional rules-based approaches often fail to keep up with increasingly sophisticated schemes – leading to high false-positive rates and overlooked threats. These static methods overwhelm compliance teams, diverting their focus from genuinely suspicious activities. Businesses need advanced systems to detect and prevent money laundering by analysing transaction patterns and network connections. For example, tactics such as money muling obscure the origin of illicit funds by layering transactions under the guise of legitimate activities. Modern AI-based tools can analyse real-time data and networks, spotting anomalies or hidden patterns that traditional systems miss. While AML regulations become more stringent worldwide, the payments ecosystem needs adaptable, effective systems to meet compliance – or risk fines and exposure to escalating threats.

Account-to-Account (A2A) scams
A2A scams, which involve payments that move directly from one account to another without using payment cards, have grown in popularity since 2020. They can stem from unauthorised account access, as seen in ATO fraud or manipulation techniques that prey on human vulnerabilities. These scams include peer-to-peer, consumer-to-business and business-to-business payment services. Following rapid growth, A2A scams are difficult to prevent.
Common risk factors include:

- Social engineering: Fraudsters trick customers into transferring funds or forfeiting sensitive information through emotional tactics, such as romance scams, investment or boiler room schemes, sextortion or impersonation scams. In the U.S., reported losses to romance scams totaled $1.14 billion in 2023.
- Authorised push payment (APP) fraud: Fraudsters deceive victims into authorizing payments under pretenses, often posing as a bank or government authority. Once the transfer is complete, victims may struggle to recover their money since they willingly authorised the transaction. Sometimes, deep fake technology mimics a loved one's voice, making the scam even more convincing. Payment and financial service providers are increasingly feeling pressure to refund victims, with proposed legislation in the U.S.25 and regulations already in place in the United Kingdom.
- Me-to-Me fraud: The scheme involves a scammer manipulating a victim into moving funds between their accounts, often across different institutions, into a single compromised account. Once the funds are consolidated into an account the fraudster controls, they steal the money.

Source: https://content.ekata.com/Trusted-Transactions-The-common-good-Creating-an-ecosystem-of-transaction-trust.html

Appendix C: Credit Card Fraud Statistics

Scheme Credit, Debit and Charge Card Fraud Perpetrated in Australia and Overseas on Australia-issued Cards

1 July 2023 - 30 June 2024

Category	In Australia		Overseas		Total	
	Transactions	Value ($)	Transactions	Value ($)	Transactions	Value ($)
Lost / Stolen	352,289	$28,893,416	177,787	$24,691,359	530,076	$53,584,774
Never Received	11,030	$1,249,831	569	$132,075	11,599	$1,381,905
Fraudulent Application	1,697	$695,865	532	$192,616	2,229	$888,481
Counterfeit / Skimming	7,603	$1,569,235	6,114	$2,136,702	13,717	$3,705,936
Card Not Present (CNP)	2,634,929	$351,176,237	2,987,975	$433,844,133	5,622,904	$785,020,370
Other	10,441	$4,230,274	9,552	$6,528,809	19,993	$10,759,082
Total	**3,017,989**	**$387,814,858**	**3,182,529**	**$467,525,692**	**6,200,518**	**$855,340,550**

Fraud Perpetrated in Australia on Cards Issued Overseas

Category	Transactions	Value ($)
Lost / Stolen	20,244	$3,171,709
Never Received	950	$183,997
Fraudulent Application	730	$102,628
Counterfeit / Skimming	25,577	$4,659,373
Card Not Present (CNP)	401,378	$75,973,533
Other	8,608	$1,972,700
Total	**457,487**	**$86,063,940**

Scheme Credit, Debit and Charge Cards Fraud Categories

- Lost/Stolen Card - fraud resulting from the loss or theft of an existing card and a transaction has taken place without the cardholder's consent or authority.
- Card Never Received - fraud where a card has been intercepted (stolen) during delivery to the customer and used before it was received by the customer.
- Fraudulent Application - fraudulent applications are applications for card accounts using a fictitious identity, using someone else's identity or providing false information during the application process.
- Counterfeit/Skimming - the use of altered or illegally reproduced cards including the replication/alteration of the magnetic stripe and changes to the details on the face of the card with intent to defraud. Skimming is a form of magnetic stripe counterfeiting in which criminals are able to copy magnetic stripe track information (including Card Verification Value - CVV) from a valid card. Information is then encoded on a counterfeit or stolen card and used fraudulently.
- Card Not Present (CNP) - the use of account information including pseudo account information without the physical card being involved, via the phone, mail, Internet etc. without the authority of the cardholder. This category also includes fraud where a card should normally be present (eg: in a retail transaction) but a merchant has chosen to accept the transaction based on a card number only and it turns out to be a fraudulent transaction.
- Other - fraud that cannot be categorised under any of the other Fraud Type categories. For example fraud using imprints of cards at merchants, or use of an existing account without the authority of the cardholder by a person who gains access to and use of the account through an unauthorized means, such as a fraudulent change of address or request for re-issuance of cards (but not lost or stolen cards).

Source: https://www.auspaynet.com.au/resources/fraud-statistics/July-2023-June-2024

Appendix D: The Role of Generative AI in Addressing Fraud

GenAI can predict card fraud from data breaches

GenAI, combined with graph technology, can detect compromised cards before fraud occurs. Mastercard's algorithm identifies merchants that may be potentially involved in breaches, analyzes recent fraudulent transactions, and checks for indicators such as pre-authorized transaction tests. GenAI can then predict the full 16-digit card numbers that are at risk and assess how likely they are to be exploited by criminals, as part of a proactive approach.[29]

Decision Intelligence Pro (DI Pro) strengthens fraud detection with GenAI

Mastercard's Decision Intelligence has long been a critical tool for transaction fraud detection. Now, with GenAI analyzing an unprecedented one trillion data points, DI Pro can more accurately predict the likelihood of genuine transactions. Based on silent performance from initial market validation against the traditional DI solution, DI Pro now captures 2X more fraudulent transactions in high score bands at a 5:1 false positive rate and identifies 30% more non-fraudulent transactions in lower-risk bands.

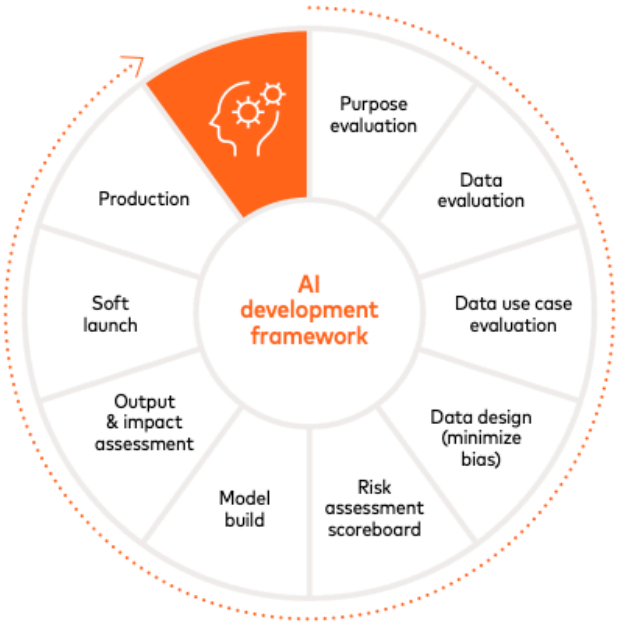
Mastercard's powerful platform: Brighterion AI

The Brighterion AI platform helps secure the payments ecosystem with advanced solutions for onboarding, merchant monitoring, and transaction monitoring across pre-authorization and post-authorization stages. Powered by global transaction intelligence, Brighterion AI solutions deliver reliable decisions that reduce fraud and risk while increasing approval rates.

Mastercard's AI governance framework

Every AI solution we create is built on an AI development framework derived from decades of experience creating proven AI solutions.

We implement a rigorous governance and review process for AI projects.[44] Mastercard uses an interdisciplinary and cross-functional approach that leverages experts in legal, privacy, product and business domains to carefully evaluate each initiative's intent, data origin and ethical implications. After a technical review evaluates scalability, return on investment (ROI), and operational efficiency, further evaluation is conducted to evaluate and mitigate risks.

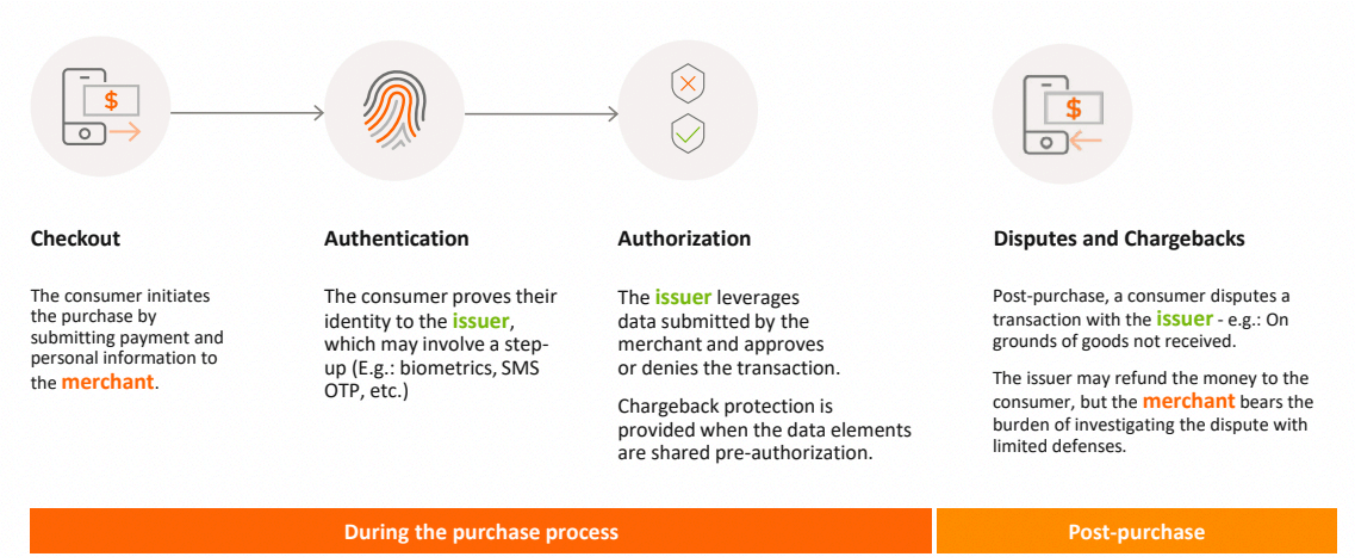


> *If it doesn't scale, it doesn't matter.*
>
> **Ed McLaughlin** | President and CTO of Mastercard

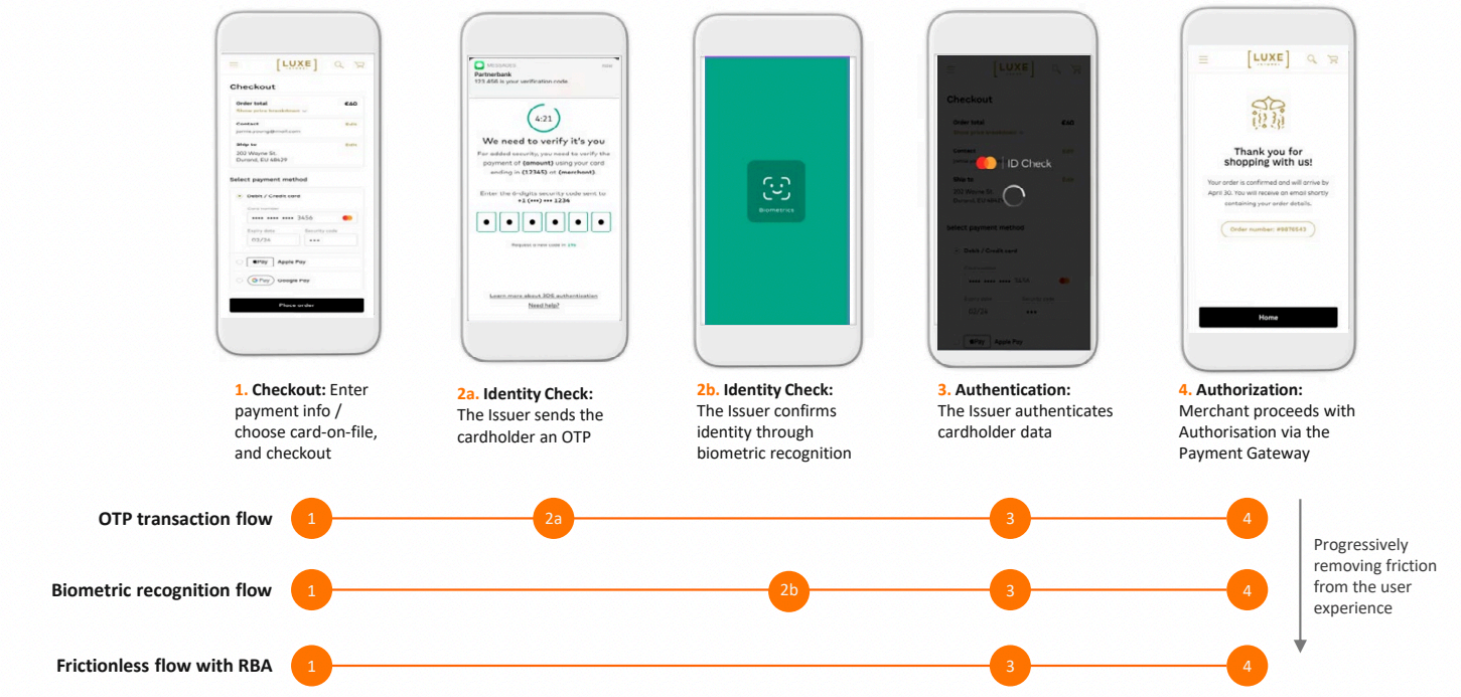
Source: https://www.mastercard.com/us/en/news-and-trends/Insights/2024/securing-the-digital-ecosystem-with-ai.html

Appendix E: Payments Purchasing Processes

Mastercard Payments Process Flow Breakdown



Mastercard Payments Process Flow Example: In-App E-Commerce Transaction



Source: https://content.ekata.com/Trusted-Transactions-The-common-good-Creating-an-ecosystem-of-transaction-trust.html

Appendix F: Mastercard Tokenisation Infographic

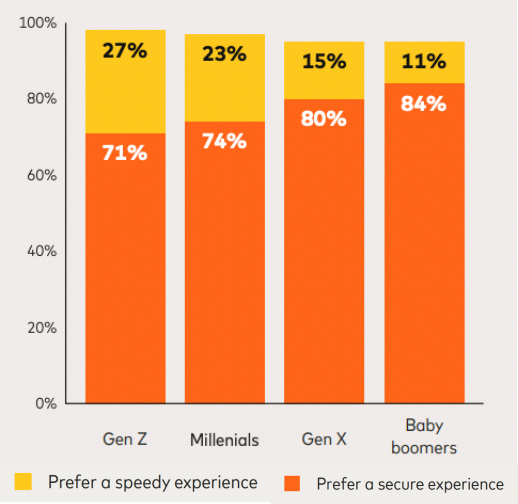
Source: https://www.mastercard.com.au/en-au/personal/get-support/safety-and-security/card-on-file-tokenisation.html

Appendix G: Consumer Trends

Broad-based Shift towards Desiring Payment Security

An important point to remember is that consumers are not 'one-size-fits-all'. Some consumers want a rapid and convenient transaction experience, whilst others (77%) are more security conscious.

Gen Z consumers are almost 2.5 times more likely to state they want a speedy online purchase journey compared to Baby Boomers. The pictured graph details that when making a purchase online, consumers prefer an experience which that is secure (but less speedy/convenient) over one that is speedy/convenient (but less secure).



Consumer Snapshot: Millennials and Gen X

Meet Nicola*

Nicola is highly tech savvy and takes her online security very seriously. She only shops at and uses platforms she trusts. Her trust is hard to build, but easy to lose. Despite strong concerns around security, she is not overwhelmingly willing to share more data with merchants or online financial institutions, even if it helps reduce fraud.

For the Nicolas's of the world...
61% are Gen X or Millennials, 55% are women

In response to their bank challenging and legitimately declining a transaction

"I forgot to alert my bank that I was traveling. It made me feel relieved because it proved to me that my bank has legitimate security measures in place to protect myself and my account".

34%
have been the victim of fraud within the last three years

68%
would be willing to share more personal data with merchants to make resolving transactional disputes more efficient

78%
would be willing to share more personal data with merchants to help reduce fraud

82%
would prefer a secure over speedy experience when making an online purchase

98%
would not use a company again if they experienced fraudulent activity when making an online purchase

Source: https://content.ekata.com/Trusted-Transactions-The-common-good-Creating-an-ecosystem-of-transaction-trust.html

Appendix G: Consumer Trends (Continued)

Consumer Snapshot: Gen Z

Meet Jason*

Jason likes to make weekly online purchases for groceries, as well as clothing. Typically, he spends around $200 online a week. When making purchases, convenience is key, and he prefers experiences which are speedy over secure. Despite his regular online spending, he has never been a victim of fraud.

For the Jason's of the world...
72% are Gen Z or Millennials, 53% are men

In response to having a transaction falsely declined

"Just made me worry about the validity of my card, and then wonder about how well their site must be run."

88%
have concerns about their personal data when making **purchases online**

43%
feel it's **absolutely crucial** they trust the merchant they're making an online purchase with when sharing personal data

97%
would be willing to share more personal data with merchants to help reduce fraud

70%
are very or extremely concerned that they'll become a victim of fraud or identity theft in the future

90%
would trust a merchant less in the future if they experienced fraudulent activities when using the platform

Consumer Snapshot: Baby Boomers

Meet Patricia*

Although not a regular spender online, she is a prolific checker of her online banking and investment apps. But when she does make online purchases, she has concerns about her personal data.

For the Patrcia's of the world...
68% are Gen X or Baby Boomers, 51% are woman

In response to having a transaction falsely declined

"It is irritating and I have changed my mind about using the site. I have also called my credit card provider to find out why"

65%
have concerns about sharing their personal data with issuers in case it is stolen and they fall victim to fraud

72%
feel it's **absolutely crucial** they trust the issuers they're sharing personal data with

74%
would be willing to share more online spending data with issuers if it helps to reduce fraud

79%
would prefer a secure over speedy experience when using an online bank or other financial service

52%
would be extremely likely to **not use a company again** if they experienced fraudulent activity when making an online purchase

Source: https://content.ekata.com/Trusted-Transactions-The-common-good-Creating-an-ecosystem-of-transaction-trust.html

Appendix H: Merchant and Issuer Trends

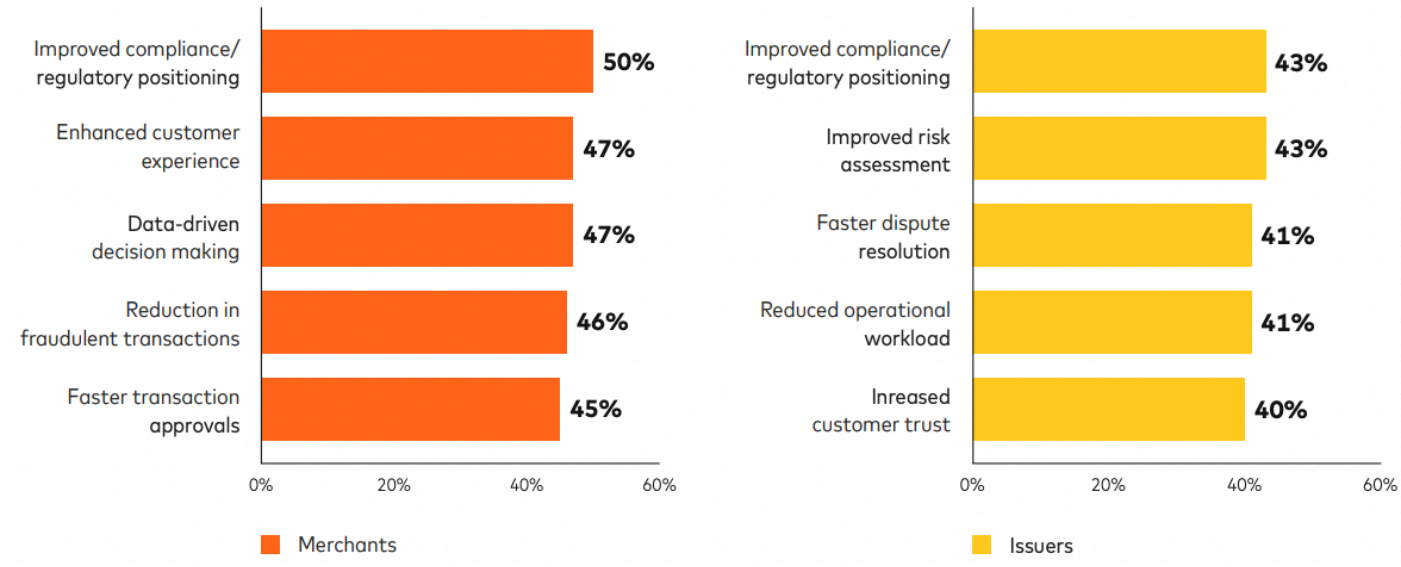
Fraud Vulnerability Among Small Businesses

Small businesses remain highly vulnerable to financial fraud, with 74% of respondents globally from a Mastercard survey expressing concern about being targeted. While this is slightly lower than the overall consumer average, the fear is especially pronounced in developing markets – 90% of small business owners in Peru, for example, reported concern. In the past year, 16% of businesses surveyed experienced financial fraud, including credit or debit card cloning (8%), stolen financial details (6%), and authorised push payment scams (9%), where victims are tricked into sending money to fraudulent accounts.

The impacts of fraud go beyond financial loss. Over half (56%) of affected respondents reported reducing their transaction activity afterward, and 40% said the experience negatively affected their relationships with family or friends – more than double the findings of Mastercard's 2019 research across Australia, the UK, and the US. As fraud cases grow more complex, financial institutions face increasing liability. This highlights the urgent need for secure, frictionless payment solutions and advanced anti-fraud tools to protect small business ecosystems and rebuild trust.

Embracement of Digital Identity Verification in Customers

Merchants and issuers alike obtain a wide-ranging array of operational benefits from implementing digital identity verification to protect their customers and associated stakeholders from fraud. Capitalising on this trend will enable new financial technologies such as Click to Pay to drive further merchant uptake.

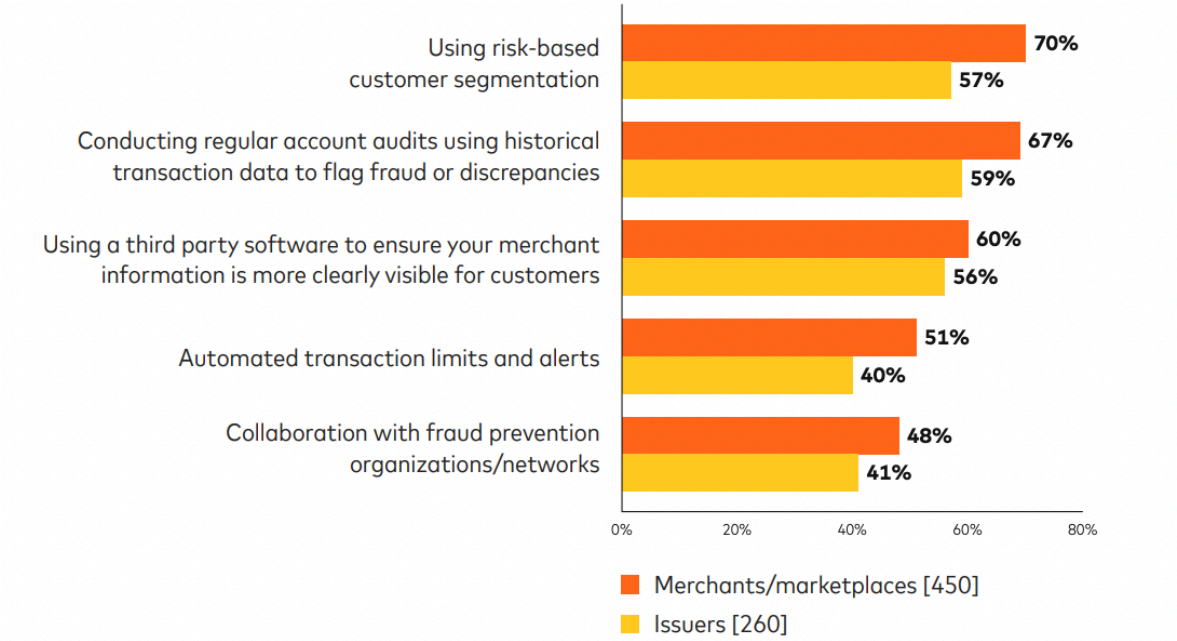


Sources: https://b2b.mastercard.com/news-and-insights/report/what-small-businesses-want-in-202021/
https://content.ekata.com/Trusted-Transactions-The-common-good-Creating-an-ecosystem-of-transaction-trust.html

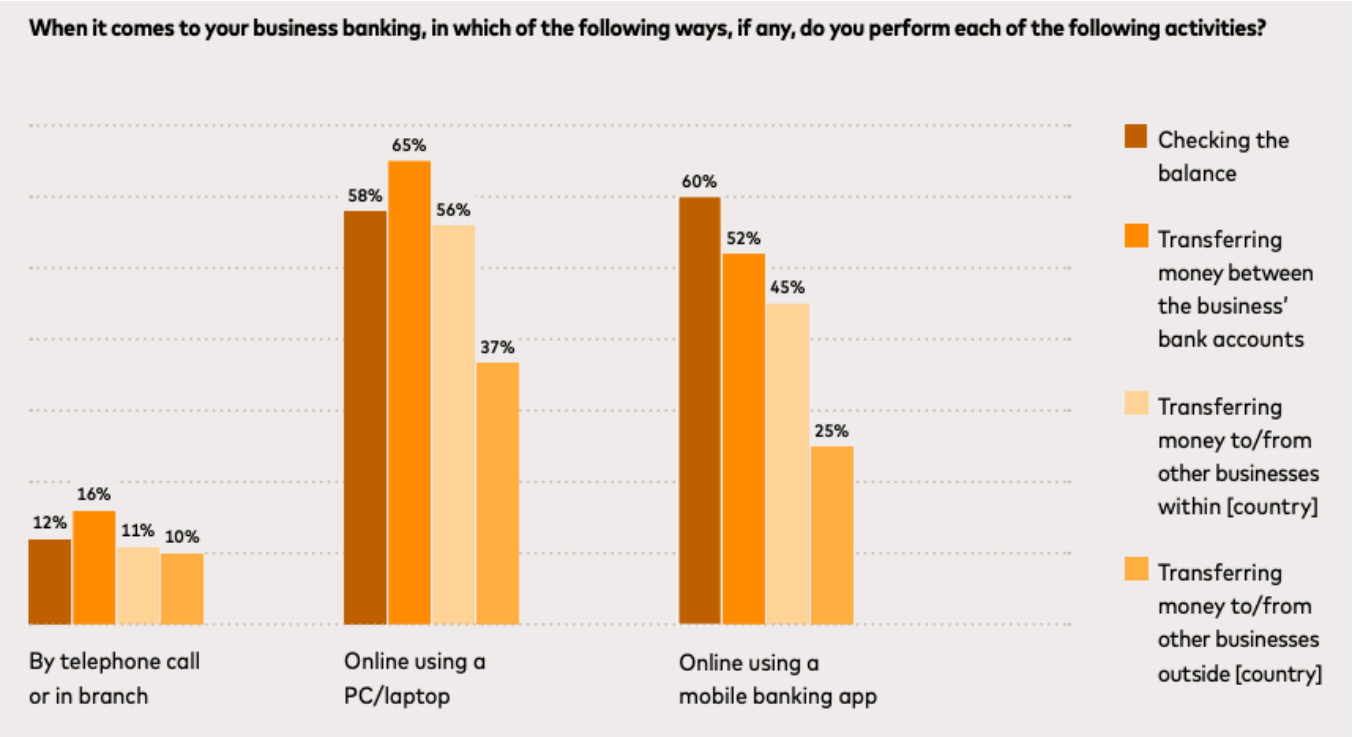
Appendix H: Merchant and Issuer Trends (Continued)

Issuers and Merchants Rely on a Broad Range of Anti-Fraud Measures

The below graph depicts the percentage of merchants/marketplaces and issuers that rely upon each following anti-fraud measure:



Platform Preferences Tailored to Business Functions



Source: https://b2b.mastercard.com/news-and-insights/report/what-small-businesses-want-in-202021/

Appendix I: Embedded Payment Ecosystems

Beyond traditional web-based checkouts, consumers are increasingly transacting within mobile applications and digital ecosystems. In these contexts – ranging from food delivery and rideshare to mobile gaming and streaming platforms – payment processes are often embedded invisibly within broader user flows. While this design approach reduces friction, it can also obscure the mechanisms of authentication and data usage. Consumers expect such systems to function securely and intuitively but often have limited visibility into when or how their payment credentials are accessed or stored. This opacity introduces another layer of uncertainty into the consumer's payment journey.

In sum, consumers are seeking payment experiences that are not only fast and convenient but also consistent, transparent, and trustworthy across contexts. Addressing these needs requires a comprehensive re-evaluation of how payment systems communicate value and security – both visibly and invisibly – through every stage of the transaction lifecycle.

Example Partner Ecosystems

Source: https://www.mastercard.com.au/en-au/personal/ways-to-pay/click-to-pay.html

Appendix J: Competitive Landscape Table

Feature/Criteria	Mastercard Click to Pay	Apple Pay	Visa Checkout / Visa SRC	PayPal	Amex Express Checkout
Ecosystem Openness	Open standard (EMVCo SRC)	Closed Apple ecosystem	Open (EMVCo)	Closed PayPal ecosystem	Closed to Amex network
Device Compatibility	All devices and browsers	Apple devices only	All devices and browsers	All devices and browsers	All devices and browsers
Tokenisation Model	Network-level (shared vault)	Device-level (on chip)	Network-level	Limited or merchant-side	Network-level (Amex only)
Authentication	Embedded: biometrics, device ID, issuer auth	Biometric (Face/Touch ID)	Issuer-defined	PayPal login/password	Issuer-defined
Merchant Integration	One-time via EMVCo SRC	Platform-specific SDK	Similar EMVCo SRC	API-based (PayPal SDK)	Limited merchant base
Brand Inclusivity	Any network, any issuer	Apple Pay only	Visa-issuer only	PayPal wallet only	Amex-issued cards only
Strategic Focus	Frictionless, secure, scalable checkout	Seamless UX within Apple ecosystem	Streamlined Visa checkout	Consumer-first digital wallet	Amex-centric loyalty UX

MASTERCARD CLICK TO PAY

Sydney International Business Competition
Case Two - 2025

Produced in collaboration with...

SIBC 2025
SYDNEY INTERNATIONAL BUSINESS COMPETITION

SCC
SYDNEY CONSULTING CLUB

THE UNIVERSITY OF SYDNEY
Business School