# Enhancing commerce to be safe, seamless and convenient

Digital Security Strategy & Roadmap in Australasia 2023

# What's inside

# Executive summary

**Australasia has witnessed massive growth in digital commerce in recent years, with technology enabling greater choice that has reshaped business. Customers demand unified commerce experiences, flexible payment methods, robust security and data privacy without added friction.**

Consumers expect every digital interaction to be intuitive and frictionless, from creating and accessing accounts through to payments and delivery, and they will take their business elsewhere when their expectations aren't met.

For all participants across the e-commerce value chain, the opportunity now is to deliver the best digital experiences at every step of the customer journey.

However, rapid growth in e-commerce has also created challenges. Cyber attacks, online fraud and scams have caused significant losses for businesses and consumers and threaten to erode trust in digital interactions.

All participants in the payments ecosystem need to play their part to anticipate and respond to the fast-changing threat landscape. This is essential to maintain a brand's reputation, the consumer's trust and to build a loyal customer base.

For business leaders today, the opportunity lies in balancing consumers' expectations for innovation and convenience against the need to deliver safe and secure experiences.

$69.4b

**was spent online by Australians and New Zealanders in 2022.[1]**

71%

**of consumers say that security is the most important element of their online experience.[2]**

80%

**increase in losses to scams reported in Australia from 2021 to 2022.[3]**

[1] Inside Australian Online Shopping, Australia Post, 2023 and eCommerce Review, New Zealand Post, 2022 (in AUD)
[2] Identity and Fraud Report: Asia-Pacific Edition 2019
[3] Australian Competition & Consumer Commission (ACCC) Targeting Scams Report 2022

# The evolving landscape

**Advances in technology including 5G networks, the proliferation of IoT devices, and the commercial application of AI have driven the growth of digital and mobile commerce.**

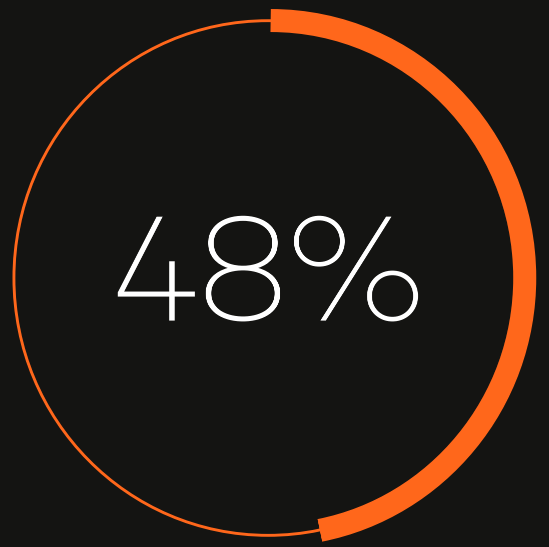
**This shift has seen Mastercard process over 126 billion in-person and online transactions.[1] At Mastercard, we're leveraging valuable intelligence from our global network data, to secure the full spectrum of digital interactions.**

We have unparalleled insights into consumers' changing expectations and behaviours, including their desire for secure digital payment experiences that exceed their expectations. Consumers want on-demand e-commerce products and services like food delivery, telehealth and omnichannel shopping to be both safe and convenient.

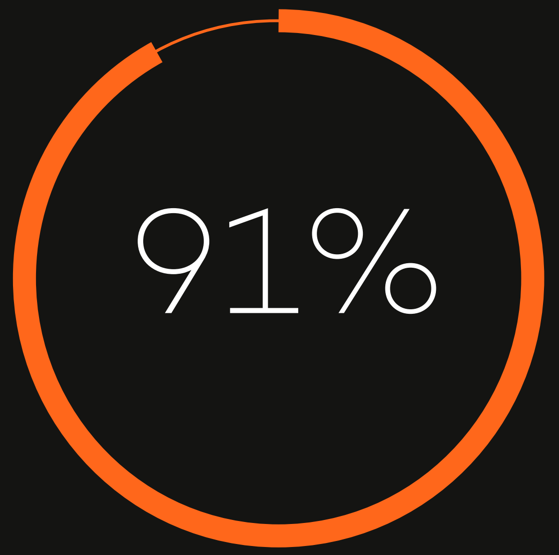
We understand the critical role we play in building a safer and best-in-class digital ecosystem. That's why we have invested in innovative technologies that leverage our global network data, to predict, detect and prevent fraud and other malicious activity.

Mastercard has the expertise and solutions needed to safeguard and enhance all stages of the consumer journey and provide secure and seamless digital experiences.

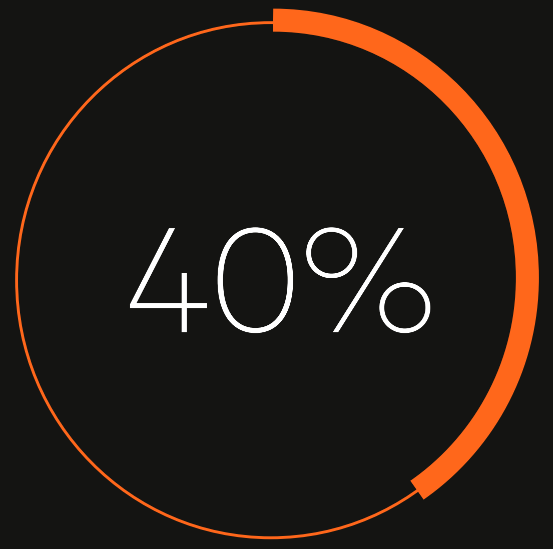
Over the last five years, we've developed and deployed a range of capabilities to reduce online fraud and help businesses flourish in the digital economy.



of online shoppers are more worried about data security now than before the pandemic.[2]



of card fraud in Australasia is from card-not-present channels.[3]



of consumers who had their transaction declined on their first visit won't try again on that merchant's site.[4]

[1] Mastercard Annual Report 2022
[2] PYMNTS Securing eCommerce Report 2021
[3] Mastercard Fraud Reporting 2022
[4] PaymentsJournal Preventing Fraud and Minimizing False Declines Nov 2021

# The journey so far

Mastercard has worked collaboratively with industry stakeholders to deliver the latest in security technologies and insights, to instil trust at every stage of the customer journey. These range from onboarding and authentication through to the post-transaction experience.

## PROTECTING PAYMENT CREDENTIALS

*Mastercard Digital Enablement Service (MDES)* protects payment data using next generation tokenisation technology. This ensures both card-on-file and on devices are encrypted and up to date, improving experiences by reducing false declines.

**5x more** Mastercard active tokens are issued in Australia than cards.[1]

## COMBATTING CARD-NOT-PRESENT FRAUD

We have adopted the EMV 3-D Secure (EMV 3DS) standard, as part of *Mastercard Identity Check* to verify consumers' identities, which helps businesses prevent unauthorised e-commerce transactions, without slowing the payment process.

Use of EMV 3DS and network tokenisation **increases approval rates by 9%+** in Australasia reducing friction in the consumer journey.[2]

## DETECTING LARGE-SCALE FRAUD EARLY

We leverage our vast global data set and Artificial Intelligence tools to actively monitor suspicious activity and block fraudulent transactions, providing a first line of defence against fraud (using *Safety Net* for Issuers and Acquirers).

*Safety Net* **blocked $13.1b in fraudulent transactions** in 2022 across Australasia.[3]

## REDUCING DISPUTES AND CHARGEBACKS

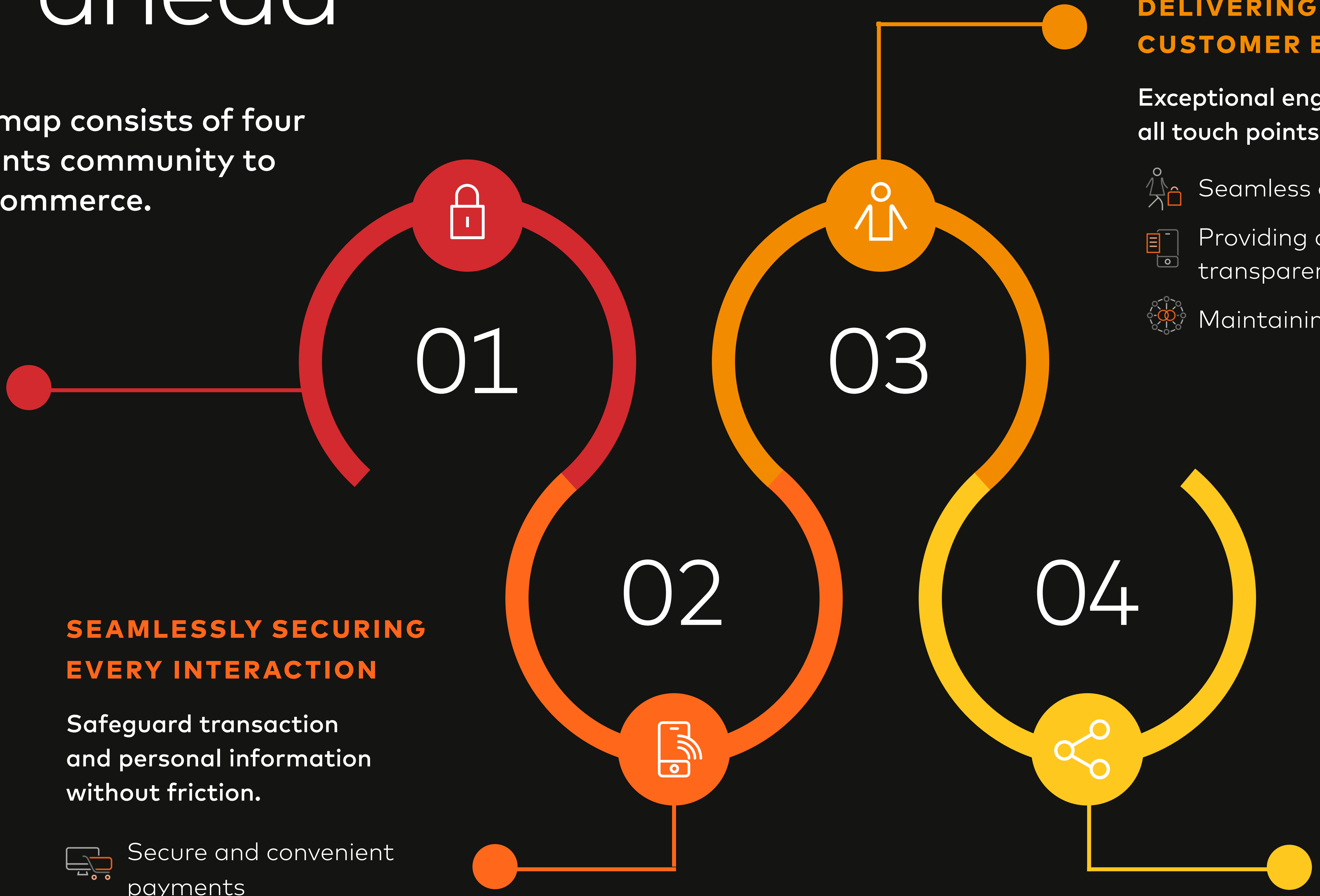
Disputes and chargebacks erode customer trust, loyalty, and net promoter scores. By combining *Mastercom* with *Ethoca*, Mastercard applies data intelligence and facilitates collaboration between financial institutions and merchants to prevent unnecessary chargebacks and enables faster resolution.

*Mastercom* has helped **reduce chargeback volumes** for issuers in Australasia by **~12%** in 2022 through early communication and resolution between issuers and merchants.[4]

1. Mastercard MDES data
2. Mastercard Q1 2023 Australasia processed data across all card types
3. Mastercard Safety Net performance FY2022 across Australia, New Zealand and Pacific Islands (in AUD)
4. Mastercom Chargeback data FY2022 Australasia

# The journey ahead

**Mastercard's Digital Security Roadmap consists of four key strategies, enabling the payments community to deliver safe, secure and seamless commerce.**



## SAFEGUARDING ACCOUNT CREATION

**Establish trust at the start of every digital interaction.**

- Seamless and secure digital onboarding
- Protecting data privacy and obtaining consent

## SEAMLESSLY SECURING EVERY INTERACTION

**Safeguard transaction and personal information without friction.**

- Secure and convenient payments
- Verifying your consumers
- Leveraging data to make better decisions

## DELIVERING GREAT CUSTOMER EXPERIENCES

**Exceptional engagement across all touch points.**

- Seamless consumer journeys
- Providing clarity and transparency
- Maintaining system resiliency

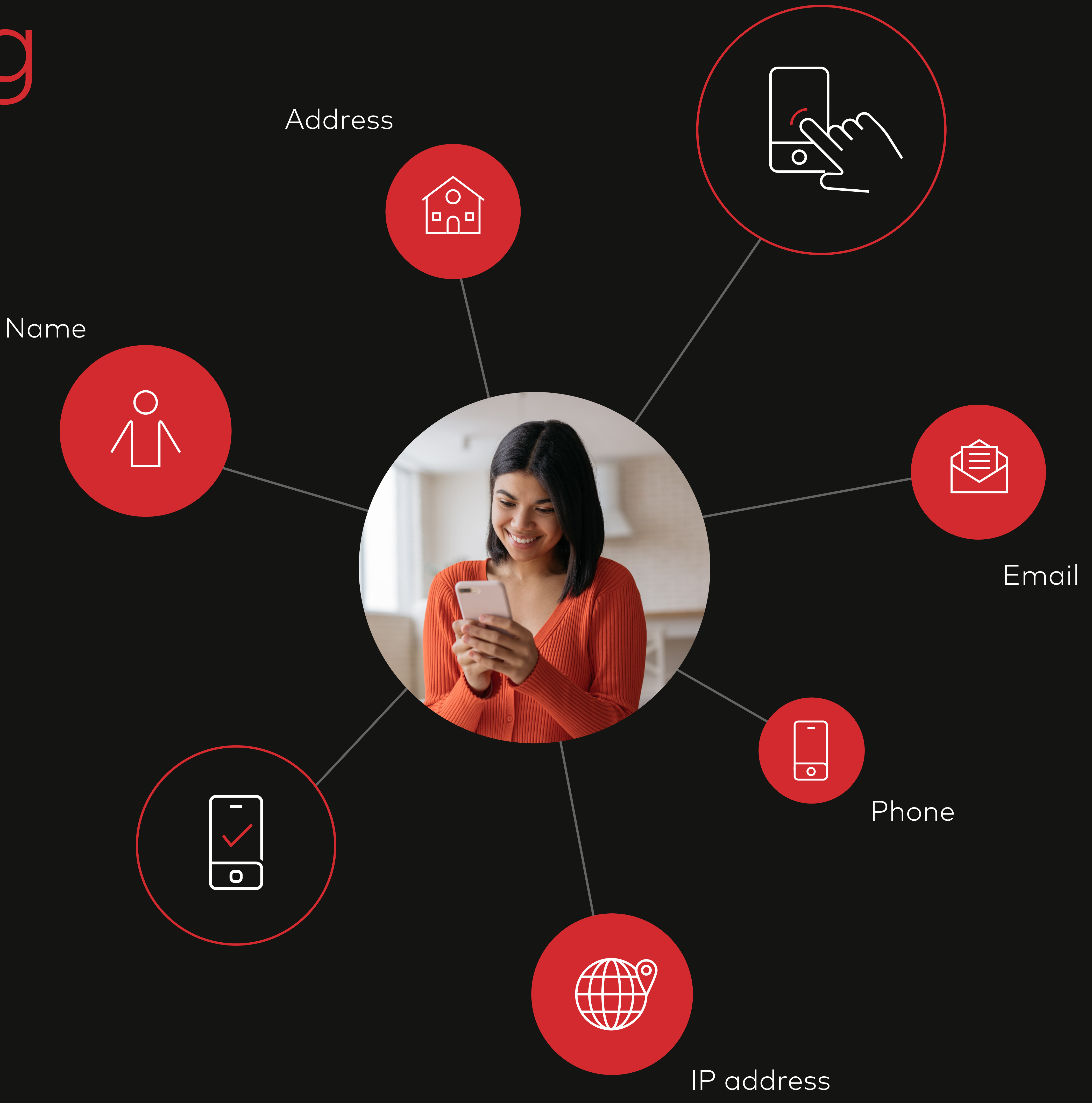
## EXPANDING SECURITY BEYOND TRANSACTIONS

**Continuous risk management across all payment rails and cyber environments.**

- Preventing cyber vulnerability
- Keeping identity credentials safe
- Preventing scams
- Delivering crypto intelligence

# Safeguarding account creation

**Mastercard aims to embed digital trust at all stages of customer onboarding, from account creation through to seamless login.**



## Seamless and secure digital onboarding

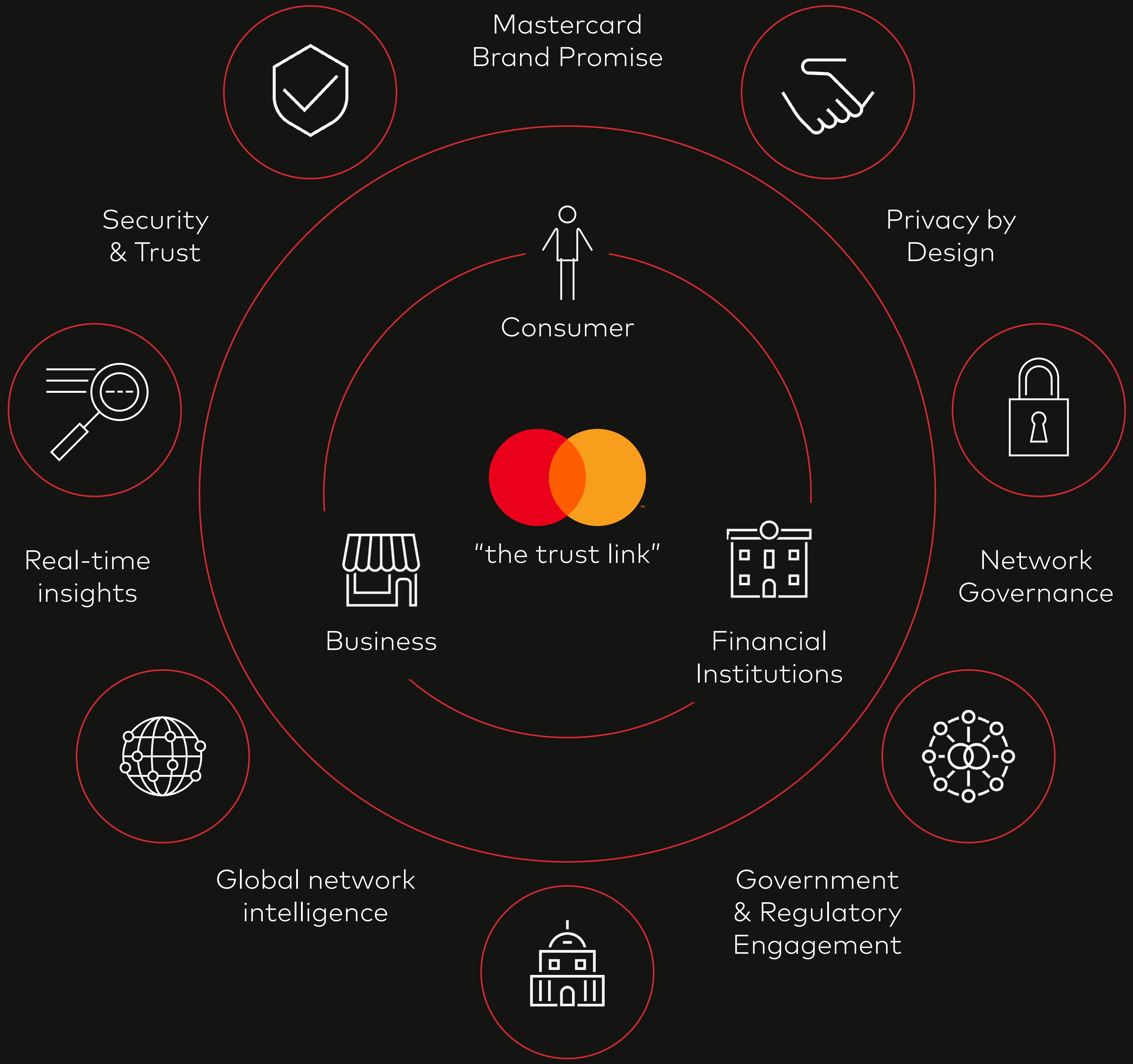
The digital ecosystem is continuing to face increased threats from the use of synthetic identity, account takeover and the use of malware and bots.

Our identity technologies can give businesses confidence that consumers are who they say they are. This is achieved by analysing identity attributes to spot inconsistencies and identify potential fraud (*Ekata*).

Businesses can also benefit from real-time intelligence harnessed from consumers' devices and behavioural biometrics (*NuData*).

And we give consumers the ability to create, manage, and use a reusable digital identity across a range of use cases (*ID: A Service by Mastercard*).

These technologies enable businesses to identify fraudulent users without added friction.



## Protect data privacy and obtain consent

We boost consumers' confidence in the security of their data by giving them greater control over how it can be shared.

Mastercard *Token Connect* enables consent-driven sharing of tokenised account and payment information between issuers and merchants. It eliminates friction and errors in the manual sign-up processes by removing the need for consumers to enter their card data or other information into the merchant's site, with their credentials held securely for a seamless purchase experience.

As different countries around the world adopt Open Banking, we are giving consumers greater control and convenience in how they share their data. By promoting the safe and secure sharing of data we are boosting businesses' confidence in how they collect payments, make credit decisions, and provide more choice to their consumers.

Mastercard is an Accredited Data Recipient under the Consumer Data Right (CDR) regime in Australia, and we've developed market-leading applications and services for the open and transparent management of consent-led data sharing.

This new service enables us to sponsor businesses to access data already held within banks, to streamline originations and promote faster and more tailored switching. Our customers can access real-time account and balance information to verify account details and perform balance checks, and to reduce mistaken payments and dishonours.

Commercial in confidence

# Seamlessly securing every interaction

**Mastercard's strategy is to secure credentials using tokenisation, improve consumer authentication using biometrics, and have more transactions approved using real-time transaction decisioning.**

## Secure and convenient payments

*Mastercard's Digital Enablement Service (MDES)* is a global best-in-class technology platform that enhances security and customer experiences in digital payments.

*MDES* uses tokenisation to replace a consumer's 16-digit card number with an alternative number or token which has specific controls regarding its use. It is a foundational platform that scales across market participants and use cases including digital wallets, merchant card on file, and guest checkout.

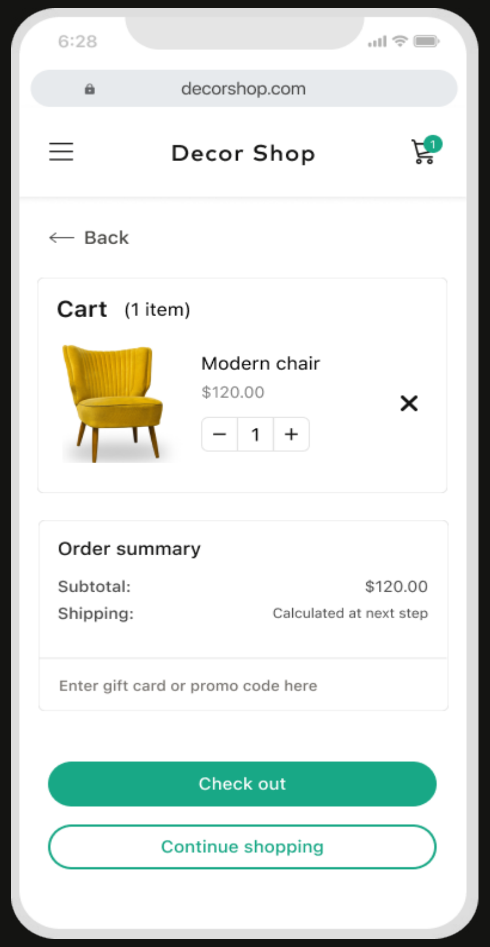
Mastercard *Click to Pay* uses *MDES* to offer a simple, secure online guest checkout experience that eliminates the need to enter sensitive payment details or passwords while still giving consumers convenient access to their cards.

*Click to Pay* provides consumers with a consistent checkout experience across devices, browsers, and applications, and its use of *MDES* tokenisation and industry EMVCo standards helps reduce fraud and preventable transaction declines. It also increases consumer trust and confidence at the time of checkout by displaying the Mastercard brand and cardholder's card art.

Layering biometric authentication on top of tokenisation further secures the online remote commerce transaction by verifying that consumers are who they say they are.

Illustrative user experience shown

1



Cart (1 item)

Modern chair
$120.00
− 1 +

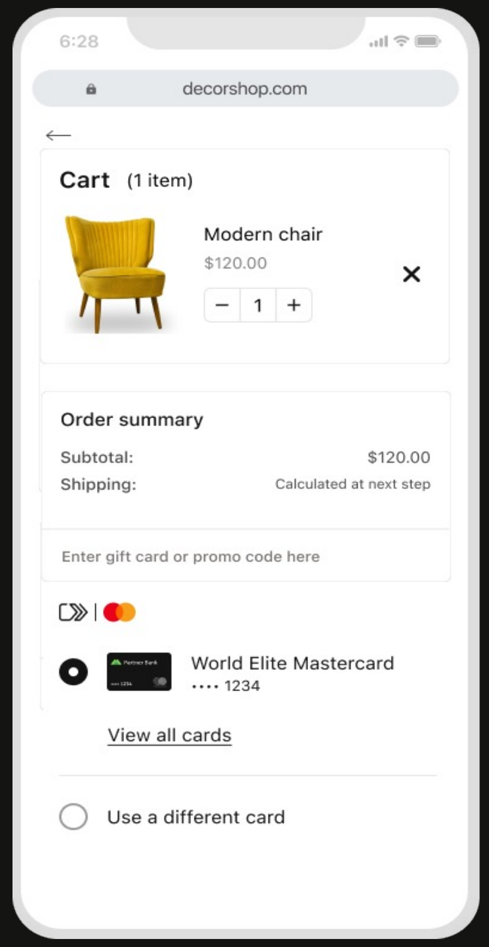
Order summary

Subtotal: $120.00
Shipping: Calculated at next step

Enter gift card or promo code here

Mastercard *Click to Pay* uses tokenisation for added security

2



Cart (1 item)

Modern chair
$120.00
− 1 +

Order summary

Subtotal: $120.00
Shipping: Calculated at next step

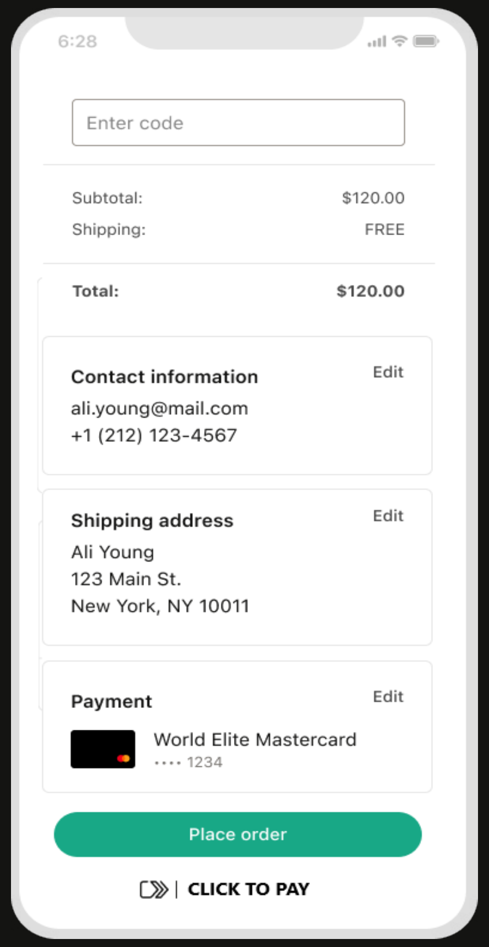
Enter gift card or promo code here

● World Elite Mastercard
•••• 1234

○ Use a different card

User is recognised and presented with available card(s)

3



Subtotal: $120.00
Shipping: FREE

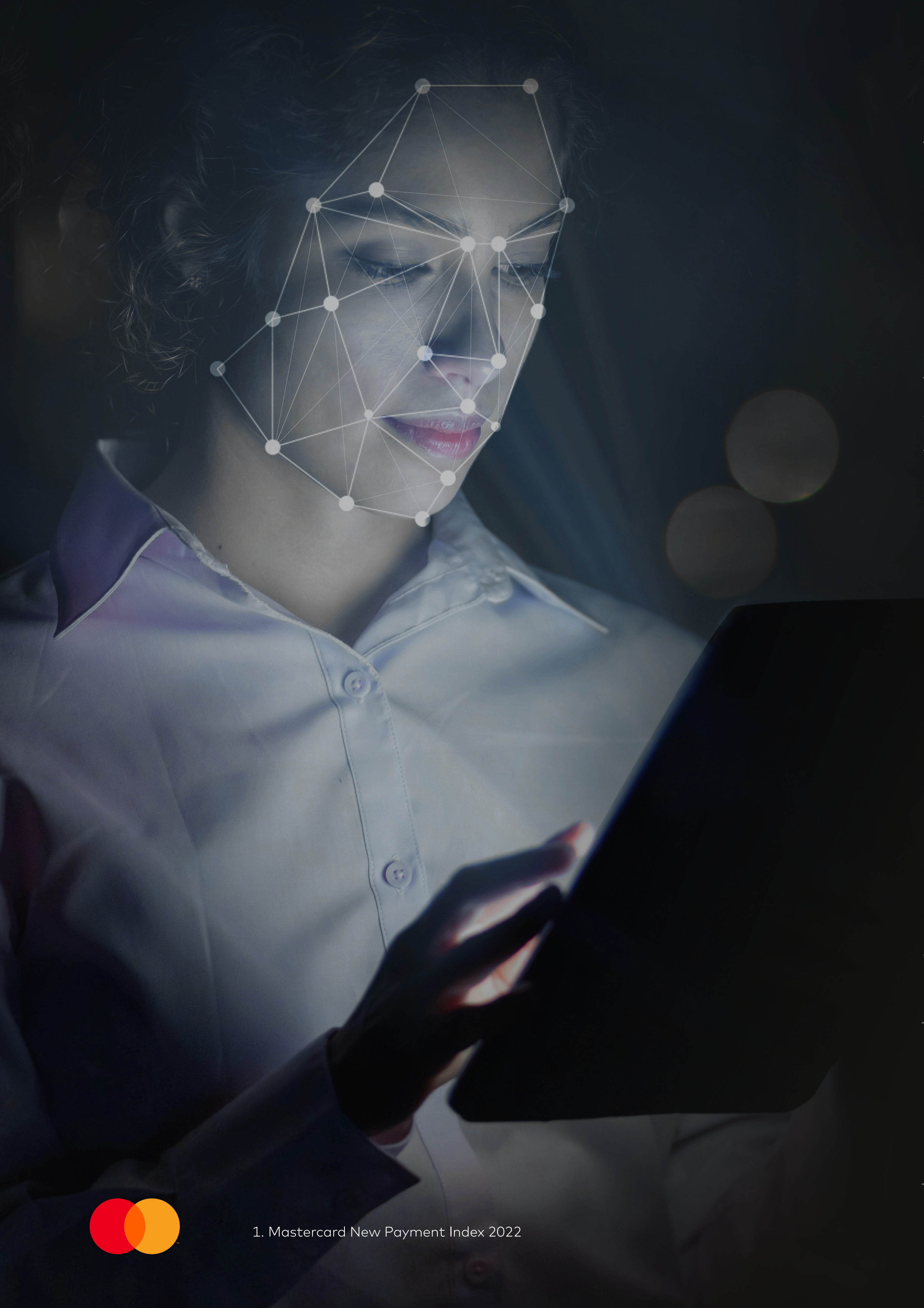
Total: $120.00

Contact information
ali.young@mail.com
+1 (212) 123-4567

Shipping address
Ali Young
123 Main St.
New York, NY 10011

Payment
World Elite Mastercard
•••• 1234

A secure checkout completed



## Verifying your consumers

The growth of digital transactions highlights the importance of deploying seamless authentication processes that also foster digital trust.

With online volumes growing, our continued focus is to address online checkout friction, fraud concerns and false declines.

This goal is achieved through the combination of tokenisation, with additional cardholder authentication services, which work together to improve conversion and consumer satisfaction while protecting businesses.

Mastercard *Token Authentication Framework (TAF)* is a comprehensive framework accessible to Merchants, Payment Service Providers and Digital Wallets to authenticate cardholders in remote commerce token transactions through, for example, *Click to Pay* or *Secure Card on File (SCOF)*. This framework leverages Mastercard's qualified or operated Multi-Factor Authentication (MFA) methods, ensuring enhanced security while reducing friction on user experience.

*Digital Transaction Authentication Service (DTAS)* is a Mastercard operated method to be used within *TAF* and provides a strong (device binding), two-factor (Fast Identity Online, Passive or EMV 3DS) authentication. The mechanism is secure, low-friction/frictionless and leveraging token capabilities.

**70% of consumers** believe that using biometrics is easier than PINs or passwords.[1]

Another way businesses can authenticate the consumer without adding friction is through Mastercard *Identity Check Express (IDCX)*, which allows cardholders to use their preferred card or token and verify themselves using device biometrics on their trusted devices (phones, tablets, laptop, etc.). *IDCX* complies with EMV 3DS and FIDO standards, helping mitigate misuse of one time passcodes.

These solutions not only ensure that user data is secure, but also create better experiences for consumers by reducing false declines, resulting in increased sales and conversion rates.

## Leveraging data to make better decisions

When the transaction is in flight (authorisation), the vast amount of data generated by the Mastercard network is used to identify and prevent fraud.

Mastercard *Decision Intelligence* combines AI and machine learning technologies, with network-level insights, to provide issuers with a real-time score on every transaction, helping them approve genuine transactions and prevent false declines.

This system continuously learns and adapts to new trends, to help issuers stay ahead of emerging threats, while improving the overall payment experience.

[1] Mastercard New Payment Index 2022

# Delivering great customer experiences

**Every business aspires to retain and build deeper relationships with customers. Therefore it is essential they deliver excellent experiences during and after the transaction, including minimising disputes and chargebacks.**

## Seamless payment processing

Consumers today have payment credentials stored with multiple merchants, digital wallets, and devices, but when these credentials expire, they can be subjected to poor experiences in the form of failed transactions.

Mastercard is creating seamless customer experiences by ensuring payment credentials are updated and accessible for all parties, delivering valuable sales to merchants and higher approval rates to issuers.

Mastercard's *Automatic Billing Updater* enables issuers to effortlessly update consumers' card credentials, preventing false declines caused by outdated card details while also notifying merchants of lost or stolen card details. These updated 16-digit card credentials are essential identifiers for issuers to approve transactions across multiple solutions, including when tokens are utilised.

Our *MDES* tokenisation solution protects sensitive customer data while giving issuers complete visibility and control of those payment credentials, simplifying provisioning and lifecycle management and reducing the likelihood of fraud and false declines.

## Maintaining system resiliency

With Mastercard, cardholders can rest assured that their card will work anywhere, any time – every time. Our *Stand-In Authorisation* service processes payments when issuer networks can't, reflecting our commitment to minimising disruption to consumers and businesses and delivering the best experiences at all times.

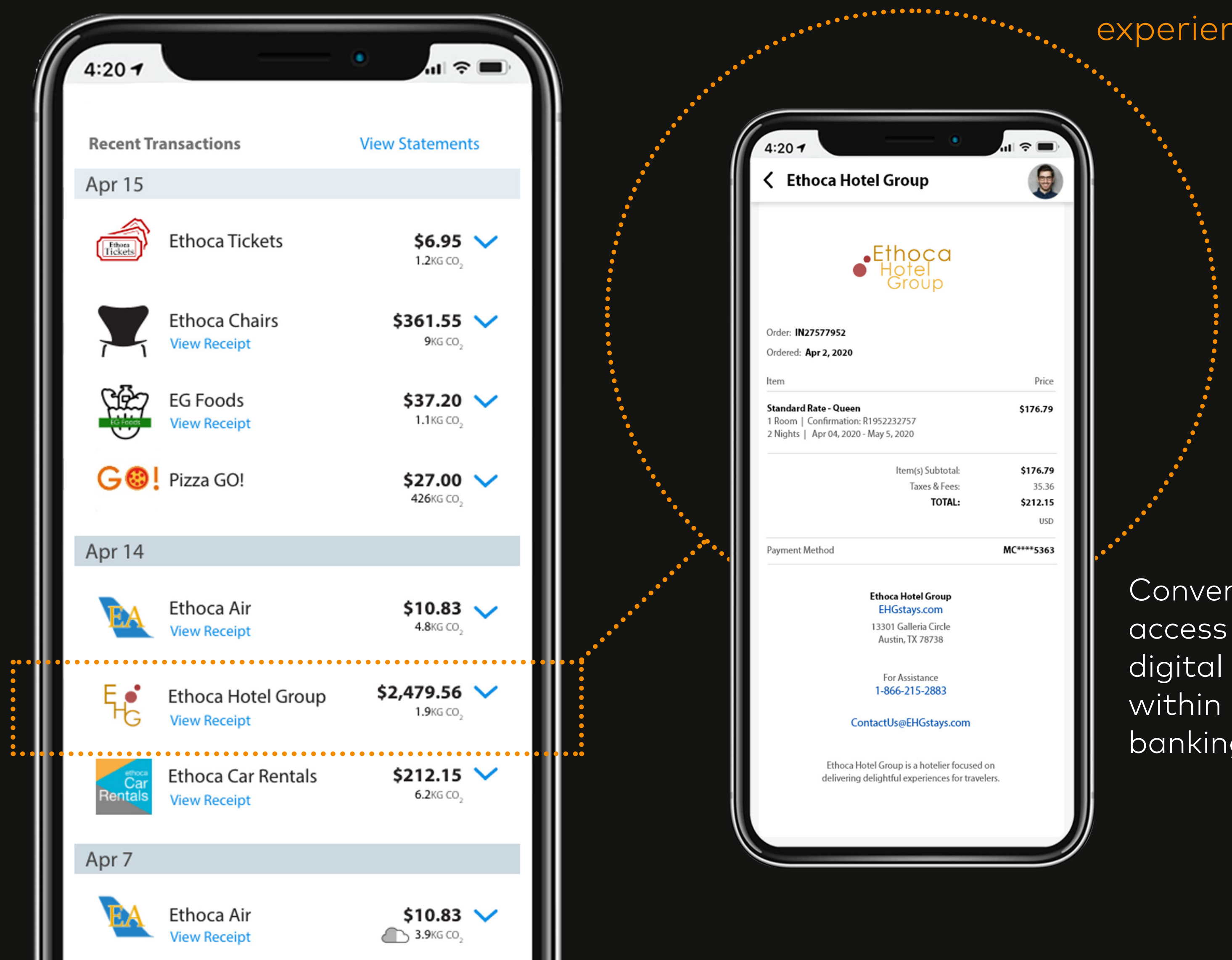
## Increased clarity and transparency

Businesses want to minimise disputes and chargebacks as they erode customer satisfaction, add operational cost and reduce profit margins.

Mastercard is collaborating with merchants and issuers to increase purchase transparency for consumers, by providing digital receipts embedded with transaction information and other details. *Ethoca Consumer Clarity* equips issuers with self-service tools to display processed transaction information via digital channels (such as online banking and bank call centres).

Providing access to better information means they are less likely to initiate disputes and chargebacks for valid transactions, helping to improve customer loyalty and retention.

Illustrative user experience shown



4:20

Recent Transactions | View Statements

| | | |
|---|---|---|
| Apr 15 | | |
| Ethoca Tickets | $6.95 | 1.2KG CO$_2$ |
| Ethoca Chairs<br>View Receipt | $361.55 | 9KG CO$_2$ |
| EG Foods<br>View Receipt | $37.20 | 1.1KG CO$_2$ |
| Pizza GO! | $27.00 | 426KG CO$_2$ |
| Apr 14 | | |
| Ethoca Air<br>View Receipt | $10.83 | 4.8KG CO$_2$ |
| Ethoca Hotel Group<br>View Receipt | $2,479.56 | 1.9KG CO$_2$ |
| Ethoca Car Rentals<br>View Receipt | $212.15 | 6.2KG CO$_2$ |
| Apr 7 | | |
| Ethoca Air<br>View Receipt | $10.83 | 3.9KG CO$_2$ |

4:20

Ethoca Hotel Group

Order: **IN27577952**

Ordered: **Apr 2, 2020**

| Item | Price |
|---|---|
| **Standard Rate - Queen**<br>1 Room \| Confirmation: R1952232757<br>2 Nights \| Apr 04, 2020 - May 5, 2020 | $176.79 |
| Item(s) Subtotal: | $176.79 |
| Taxes & Fees: | 35.36 |
| **TOTAL:** | $212.15<br>USD |
| Payment Method | MC****5363 |

**Ethoca Hotel Group**
EHGstays.com
13301 Galleria Circle
Austin, TX 78738

For Assistance
1-866-215-2883

ContactUs@EHGstays.com

Ethoca Hotel Group is a hotelier focused on delivering delightful experiences for travelers.

Convenient access to digital receipts within issuer banking app

# Expanding security beyond transactions

**Mastercard has decades of experience protecting the card network and we aim to extend our security capabilities to protect all other transactions.**

Digital channels offered a lifeline to businesses during the pandemic but security was not always their top priority.

We saw a rise in the number of data breaches in Australia as hackers profited from businesses that were unprepared and unaware of the risks.

**20% of the large-scale data** breaches in Australia involved a breach from third-party service providers.[1]

With this compromised data, criminals created fraudulent accounts, and logged on using stolen credentials, creating downstream impact and an increase in payment fraud.

## Preventing cyber vulnerability

Cybersecurity is an important part of the digital strategy. Continuous monitoring and assessment of cybersecurity will help mitigate against large-scale cyber attacks and data compromises, and preserve the strong brand value and reputation that businesses have earned.

Mastercard can help businesses proactively assess and monitor the risk exposure in your organisation or from vendors, consultants and suppliers that have access to your systems and data, using *RiskRecon*, that identifies vulnerabilities with third parties, to help protect businesses.

## Keeping identity credentials safe

**1 in 4 Australians** have been a victim of identity theft at some point in their lives.[2]

Mastercard is committed to keeping the identities of consumers safe, using proactive techniques such as identity monitoring.

We give consumers control of their identity by providing detection and protection against identity theft, including monitoring and alerts, together with self-service tools that help them take preventive action *(Mastercard ID Theft Protection)*.

[1] Australian Cyber Security Centre (ACSC) Annual Cyber Threat Report July 2021 to June 2022 (FY2022)
[2] Report/survey by Australian Institute of Criminology (AIC)

## Preventing scams

Scams are a major global issue. Lack of data and intelligence to prevent the scams before they happen exposes ecosystem participants to financial losses.

Scams represent a significant risk for the economy, with Australians and New Zealanders **losing a record $3.1b to scams** in 2022.[1]

Mastercard can help mitigate scams and money mule activity on account-to-account payments by providing pre-payment risk assessment before funds are transferred to a fraudulent account.

Mastercard's central role in the global payment ecosystem means we have clear visibility of evolving criminal activity. We utilise these insights alongside artificial intelligence, to detect scams in real-time and prevent money laundering.

## Delivering crypto intelligence

Once a scam is executed, criminals take advantage of the increasing speed and ease with which money can be moved between accounts or buying cryptocurrencies.

To mitigate this risk, Mastercard acquired *CipherTrace* which provides businesses with comprehensive insights and visibility into cryptocurrency transactions. This can be used to identify the potential risks associated with various exchanges based on their KYC measures, privacy coins, and involvement with dark web marketplaces.

Mastercard can also provide tools to identify and trace illicit funds moving across the entire network. This enables you to uncover and alert suspect mule accounts and stop fraud faster, with more accuracy.

These tools provide reporting and analytics which can be used for regulatory compliance, thereby promoting trust and transparency in cryptocurrency transactions.

Investment scams in Australia and New Zealand in 2022 were **over $1.5b**, with cryptocurrency being the most common payment.[1]

Commercial in confidence

[1] Australian Competition & Consumer Commission (ACCC) Targeting Scams Report 2022, and Cert NZ 2022 Report (in AUD)

# Playing your part to protect the ecosystem

| | 01 SAFEGUARDING ACCOUNT CREATION | 02 SEAMLESSLY SECURING EVERY INTERACTION | 03 DELIVERING GREAT CUSTOMER EXPERIENCES | 04 EXPANDING SECURITY BEYOND TRANSACTIONS |
|---|---|---|---|---|
| **MERCHANTS** | • Prevent account takeover by utilising passive biometrics, liveness detection and consent-driven data sharing, for a secure and seamless digital onboarding experience to consumers. | • Maximise approval rate (and sales) with a combination of tokenisation and payment authentication.<br>• Reduce fraud without adding friction by leveraging with biometrics. | • Reduce potential chargebacks by increasing transparency on transactions.<br>• Maximise approvals/sales by leveraging updates of payment credentials. | • Continuously monitor the cyber health of your own organisation and that of your third-party suppliers. |
| **ACQUIRERS & THIRD-PARTY SERVICE PROVIDERS** | • Assess business risk during onboarding.<br>• Equip businesses with tools to verify and onboard customers without friction. | • Help businesses minimise fraud and risk with solutions like tokenisation and payment authentication with biometrics. | • Offer businesses tokenisation and lifecycle management tools to reduce preventable declines. | • Continuously monitor the cyber health of your own organisation and that of your third-party suppliers. |
| **ISSUERS** | • Protect consumer identities and streamline onboarding with real-time identity intelligence and secure data sharing. | • Secure payment credentials with tokenisation.<br>• Verify customers with device-based biometrics and digital identity signals.<br>• Utilise real-time transaction decisioning tools to increase approvals. | • Provide customers with self-service tools to review transactions and reduce dispute volumes.<br>• Reduce preventable declines using tokenisation and lifecycle management tools. | • Continuously monitor the cyber health of your own organisation and that of your third-party suppliers.<br>• Empower consumers to know and respond if their identity has been breached and avoid scams.<br>• Provide security across new payment rails like crypto and account to account. |

# In summary

At Mastercard, we work to connect and power an inclusive digital economy that benefits businesses and consumers by making transactions safe, simple, smart and accessible.

We have been investing in innovative technologies to capitalise on emerging trends whilst mitigating new threat vectors.

Balancing the desire for exceptional experiences against the need for maximum security is an ongoing mission – one where there is no room for compromise on either side of the equation.

Executing this mission requires all parties to come together and develop and adopt best-in-class technologies. Together we can build a safer and inclusive digital world.

This document contains the proprietary and confidential information of Mastercard International Incorporated and/or its affiliates ("Mastercard"). The contents of this document and the fact and substance related to the existence of this document are confidential and proprietary information of Mastercard. You shall not disclose the contents of this document or discuss its existence with any third party or use this document in any manner other than in connection with the evaluation of the opportunity described herein with Mastercard. You shall limit dissemination of this document within your company only to those employees or officers who have a need to know for the purposes of evaluating such opportunity.

This document is intended solely to facilitate discussion between the parties and does not create a legally binding or enforceable offer or agreement (except for the confidentiality obligations set forth above). This document only sets forth certain information regarding the financial and other terms that are anticipated to be included in a proposed agreement between the parties, and not a complete description of such terms. The parties acknowledge that other standard terms and conditions are also anticipated to be included in the proposed agreement. Except for the confidentiality obligations set forth above, neither party shall be liable to the other party as a result of the failure to fulfill any obligation described in this document or the failure to enter into any agreement contemplated by the original request for proposal or our response thereto.

All brands, logos, trade names and marks referred to herein ("Trademarks") are the property of their respective trademark holders. Mastercard does not make any claims in relation to any third-party Trademarks. Any references to such Trademarks in this document are for informational purposes only, and do not constitute any affiliation, endorsement and/or sponsorship of the Trademarks, the underlying products, and/or the Trademark holders. You are solely responsible for seeking the prior consent of the Trademark holder for any use of a Trademark.

In addition, information in this document or in any report or deliverable provided by Mastercard in connection herewith relating to the projected impact on your financial performance, as well as the results that you may expect generally are estimates only. No assurances are given that any of these projections, estimates or expectations will be achieved, or that the analysis provided is error-free. You acknowledge and agree that inaccuracies and inconsistencies may be inherent in both Mastercard's and your data and systems, and that consequently, the analysis may itself be somewhat inaccurate or inconsistent. The information, including all forecasts, projections, or indications of financial opportunities are provided to you on an "AS IS" basis for use at your own risk. Mastercard is under no obligation to update this information and you are solely responsible for your use of the information as well as any decision or action you take as a result of this document, or any inaccuracies, inconsistencies, formatting errors, or omissions.

Commercial in confidence

# Contact

For any questions, please speak to your account manager or email Mastercard.Digital.Security.ANZ@mastercard.com