JANUARY 2024

THE UPDATE

Connecting you to the best insights, latest news and emerging trends in innovation, cyber and security

MASTERCARD ACCESS

How a services network helps customers streamline innovation and increase efficiencies

INSIDE THIS EDITION

Access + Cyber + Identity + Risk & Resiliency

Foreword

Ajay Bhalla
President, Cyber &
Intelligence, Mastercard

Welcome to our second edition of The Update.

In today's dynamic digital economy, payments need to take place at the speed of a click and behind-the-scenes critical elements from security to loyalty need to seamlessly align in real time.

Yet as we all enjoy an expanding choice of payments options, which adds levels of complexity for payment providers, whereas people's expectations for safe and flawless payment experiences have only increased.

In this issue of The Update, we take a deep dive into the considerations that go hand in hand with the expansion of payment choice. We have gathered insights from across Mastercard's Cyber and Intelligence business to help you navigate the intricate challenges we face from today's rapidly evolving digital payments landscape.

We ask the questions: What if you had access to the services you need via one single connection to multiple card networks and payment rails? And what if you could deploy one solution for each need that can work across Mastercard branded and nonbranded transactions?

We understand these are pain points for many of you and with this knowledge we have built Mastercard Access, a scalable, fast, secure and trusted single connection to a services network. Where choice matters, simplicity is assured, and security is paramount.

Thank you for taking the time to read our newsletter — and for your ongoing partnership. In an era that continues to be defined by rapid innovation, I firmly believe that it is you, our partners and customers, who are central to the progress we collectively make in keeping security and trust at the heart of a vibrant digital world.

Ajay Bhalla

Contents

ACCESS

05 Mastercard expands access to innovation and cutting-edge services via single trusted connection →

08 Adapting collaborative AI for improved fraud detection and customer experience →

11 Seamless and secure: Embracing account-to-account payments with Mastercard Access →

14 Delivering a curated services journey with ubiquity and trust in every interaction →

16 Mastercard Access: Elevating customer experience across Europe through innovation →

CYBER

19 Deep currents: What you need to know on managing supply chain risk in 2024 →

22 Why chargebacks are changing →

26 The nature of fraud in fiat and crypto currencies →

IDENTITY

32 How online retailers can fight fraud during the sales season →

35 Preventing promo abuse: Online retailers' fastest growing risk →

39 Fighting first-party fraud to retain trust and avoid chargeback misuse →

RISK & RESILIENCY

42 AI can help banks sharpen payment resiliency and maintain consumer trust →

44 Transaction risk management technology secures the digital financial environment with Saudi Awwal Bank →

46 Navigating sophisticated transaction fraud trends in 2024 →

49 Sustainable cards for an environmentally conscious future →

51 Mastercard's RiskX: Navigating the future of cybersecurity and trust →

ACCESS

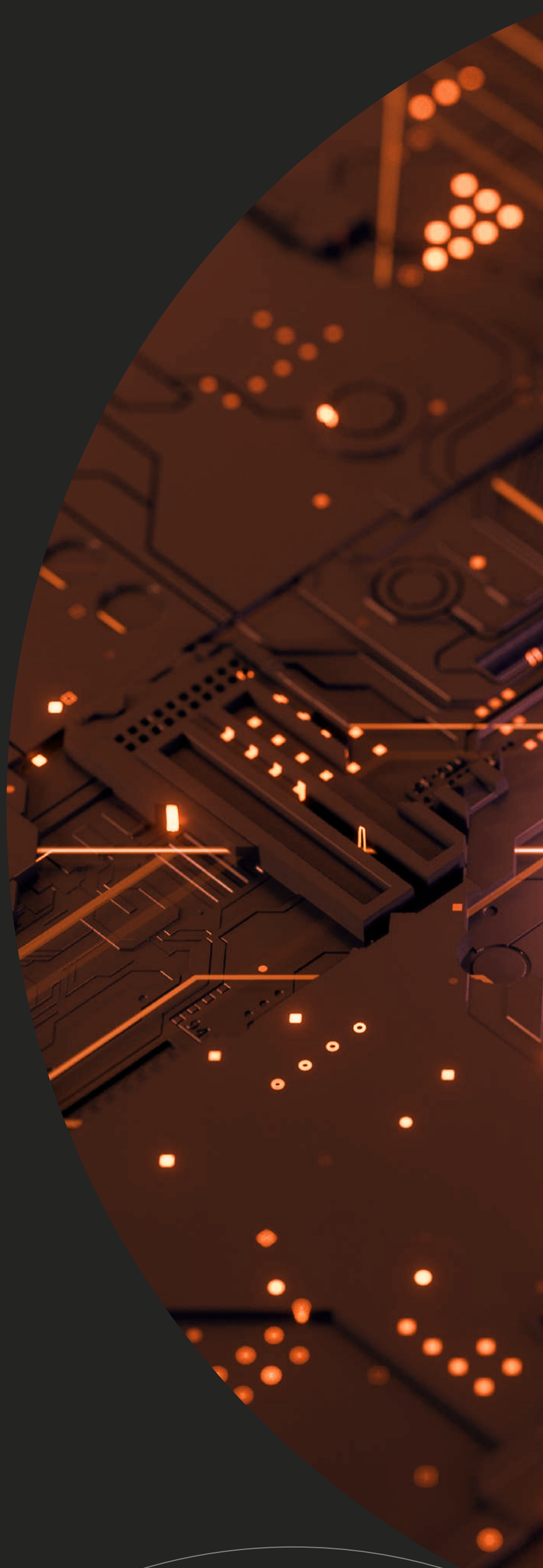
05 Mastercard expands access to innovation and cutting-edge services via single trusted connection →

08 Adapting collaborative AI for improved fraud detection and customer experience →

11 Seamless and secure: Embracing account-to-account payments with Mastercard Access →

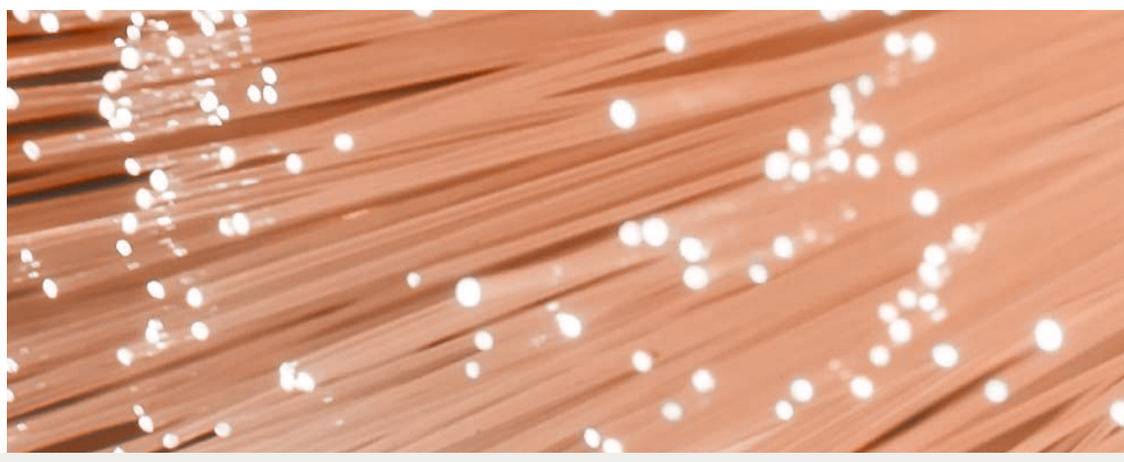
14 Delivering a curated services journey with ubiquity and trust in every interaction →

16 Mastercard Access: Elevating customer experience across Europe through innovation →



Mastercard expands access to innovation and cutting-edge services via single trusted connection

Kaushik Gopal
Executive Vice President,
Access Solutions/Revenue
& Sales Enablement



Introducing Mastercard Access: A single trusted connection to a services network

Mastercard Access is the latest extension of our payments network and a new trusted connection into an innovative services network. It allows for a simple, cost-efficient, single point of access to services traditionally only seen on Mastercard-processed transactions — yet now made available through customers' existing payments infrastructure and across multiple rails or networks, providing a holistic experience across a customer's portfolio.

Mastercard has a rich history of pioneering technology to make payments simpler, smarter and safer. Now the company is expanding its network further — beyond payments — to empower customers with swift, consistent and seamless access to a suite of services designed to accelerate innovation.

This first-of-its-kind offering provides a trusted point of connection where customers can benefit from global scale, artificial intelligence-driven insights, risk mitigation, improved experiences and other value-added Mastercard solutions. In the same way they might download an app on a mobile device, it's simple, secure and convenient. All of this is not only limited to Mastercard's suite of services but also includes access to third-party services going forward.

Mastercard has a rich history of pioneering technology to make payments simpler, smarter and safer.

Streamlining access to market-leading services

In today's dynamic digital payments landscape, the abundance of technology options and payment service providers has raised expectations for seamless, secure transactions.

Consider the evolving role of chief technology officers, who are now tasked with implementing multiple platforms that support efforts on fraud prevention and business optimization. Traditionally, CTOs sourced, deployed and financed solutions tailored to specific payment rails, or products, resulting in a complex development pipeline.

This digital proliferation not only brings significant opportunities for optimizing operations, forecasting and planning but also reveals that the vast majority (71%)[1] of businesses prioritize cost-efficiency. To enable innovation, businesses must tackle the challenge of selecting and accessing market-leading solutions, while reducing time and money spent on complex implementations.

The services network available through Mastercard Access addresses these challenges simultaneously; cost, scalability, speed and security, all through a single connection across multiple rails.

This approach empowers businesses to subscribe to services at a unit cost, tapping into Mastercard's significant investments in AI-driven services and digital innovation, thereby enhancing performance, reducing costs and improving overall profitability.

Organizations also benefit by freeing up resources to focus on priority initiatives instead of wasting time on implementation and management. This also makes it easier for businesses to scale and streamline technology adoption with solutions that embody trust, innovation and intelligence that Mastercard has built through its commitment to Privacy by Design.

Lowering the cost of innovation to future- proof the ecosystem

Businesses no longer need to invest in disparate and disjointed ecosystems. Working with Mastercard offers partnership with an industry leader that has already invested billions in the future of digital security, both in payments and beyond. Despite organizations setting cost reduction goals, 81% are unable to fully achieve them.[1] This is often attributed to rationalizing high expenses involved in using, implementing and managing services. Additionally, some organizations unintentionally pay multiple vendors in their technology stack for the same service, leading to unnecessary additional costs. Another hindrance to cost reduction is the approach organizations take in adopting new technology. Building an in-house capability to connect solutions across various vendors can be costly and time-consuming, contributing to elongated timelines.

Instilling trust into every interaction

More than ever, consumers are concerned with how their personal data is being managed and protected. Mastercard's vast global network intelligence is key to the development of Mastercard's advanced technologies, making them best-in-class solutions. This intelligence is derived from anonymized and aggregated transaction data, ensuring personal data and privacy remains just that — personal and private.

Mastercard's payments network is trusted by businesses and consumers globally. Trusted to make safe, secure payments, trusted as a technology leader, and trusted for its data and privacy practices. Through Mastercard Access, this same trust extends to a services network, underpinned by the same safety and security that customers experience with Mastercard every day.

Solutions made available to customers via Mastercard Access include Safety Net, which provides network-level protection against large-scale fraud attacks; Decision Intelligence, a real-time authorization decision-making solution; and Mastercard Digital Enablement Services, a collection of on-behalf services to allow issuers to support wallets and remote commerce programs to process tokenized transactions.

Today, Mastercard Access is available to all industry players, and via one single connection, customers can future-proof their businesses and leverage the unique benefits that Mastercard can help them realize.

Adapting collaborative AI for improved fraud detection and customer experience

Rohit Chauhan
Executive Vice President, Artificial Intelligence

For decades, industry leaders have been finding ways to apply artificial intelligence (AI) and machine learning (ML) to cybersecurity solutions.[2] At the same time, cybercriminals have been evolving their techniques to keep up with these defenses. Players in the payments industry know that innovation is a must to stay on the cutting edge of technology.

We've seen some tremendous innovations regarding AI's power and its ability to prevent fraud in real time and improve customer experiences. According to Javelin Strategy and Research's 2022 Identity Fraud Study,[3] there was a 109% year-over-year increase of new account fraud in 2022, but the same study[4] reported a 42% decline in losses attributed to new account fraud in 2023. So, the question is, what changed to stop the onslaught of fraud?

These findings suggest that as organizations responded to new threats by adapting their security tools and strategies to better combat new account fraud, they were able to stem the tide. To stay ahead of the rapidly evolving fraud landscape, it's important to quickly adopt emerging security tools. This underscores the critical role of accessing and quickly deploying solutions to keep pace with the velocity of change.

Harnessing the power of AI

Through Mastercard Access, we are making it easier and more convenient to facilitate this process via a single trusted connection to a services network. These offerings go beyond payment solutions to create a cohesive ecosystem where customers can leverage a variety of interconnected tools, including AI-driven, intelligent insights to protect their ecosystems from cybersecurity threats.

Let's look at some specific examples that illustrate how AI is fueling the innovative fraud detection models that are helping organizations safeguard customer data today.

Constructing digital neighborhoods: The evolution of fraud management

Data-driven intelligence helps us understand risk and empowers us to make safer and smarter choices in our day-to-day lives. And with the power of AI insights and data analysis, players in the payments industry can create more detailed transaction profiles than ever before. They can build "neighborhood" transactions in a profile, opening new data points for deriving insights, improving customer experiences and defending ecosystems against fraud threats.

Today's Decision Intelligence fraud models map the entire transaction database so that the risk factors of merchants and consumers are compiled to provide a 360-degree view. The ability to view data in this holistic manner opens new possibilities to analyze card transactions and provide an improved customer experience that removes friction and keeps fraud at bay.

Think of the neighborhood like this: As consumers interact with merchants, the transaction is logged, building a virtual map of the merchants in different geographic locations. Often, when one merchant experiences fraud, other merchants in that neighborhood also tend to see fraud. This new dimension of insights makes fraud much more manageable to proactively alert merchants and consumers to potential threats.

Nexi Group and the power of collaborative AI

Nexi Group, one of the leading processors in Europe, is on a mission to solve the problem of fraud in its operations. Its application of Decision Intelligence and Safety Net solutions via Mastercard Access exemplifies the power of collaborative AI in fraud management. Integrating consortium models with these tools, Nexi accesses extensive fraud data, enhancing its detection and prevention capabilities and showcasing the effectiveness of shared intelligence in combating fraud threats.

Giovanni Bruner, head of fraud intelligence & modeling at Nexi Group says, "The integration of these advanced tools has significantly bolstered our ability to preempt and combat fraud, providing invaluable insights in our ongoing efforts to protect our customers." The agility and collaboration of fraudsters necessitates a similar cooperative approach among all financial institutions to facilitate effective sharing of fraud-related information. Mastercard's comprehensive analytical models, including graph-based analytics, provide Nexi with a broad view of consumer transactions. This collaborative approach is essential in identifying and combating emerging fraud patterns, while also leveraging AI for enhanced consumer protection.

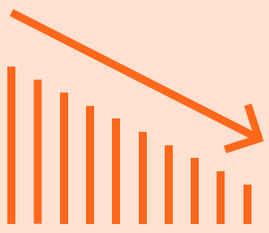
The agility and collaboration of fraudsters necessitate a similar cooperative approach among all financial institutions to facilitate effective sharing of fraud-related information.

Reducing fraud and improving success through the network access facilitation layer

When fighting fraud, there is no single solution to address the entire threat landscape. Instead, organizations can use Mastercard Access, which provides a facilitation layer to reach numerous tools under one roof.

This brings multiple benefits and helps payment service providers make sure that their ecosystems are future-proofed as we continue to see higher volumes and new types of fraud.

> **When fighting fraud, there is no single solution to address the entire threat landscape.**

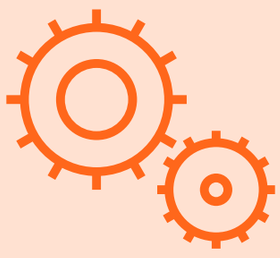


Reducing fraud

With a services network that provides a 360-degree view of customers, richer profiles and neighborhoods are seen, which results in reductions in fraud.

Improving profitability

Equipped with richer insights, we're able to make more accurate transaction approval decisions. Approving more transactions directly contributes to boosting customer profitability.

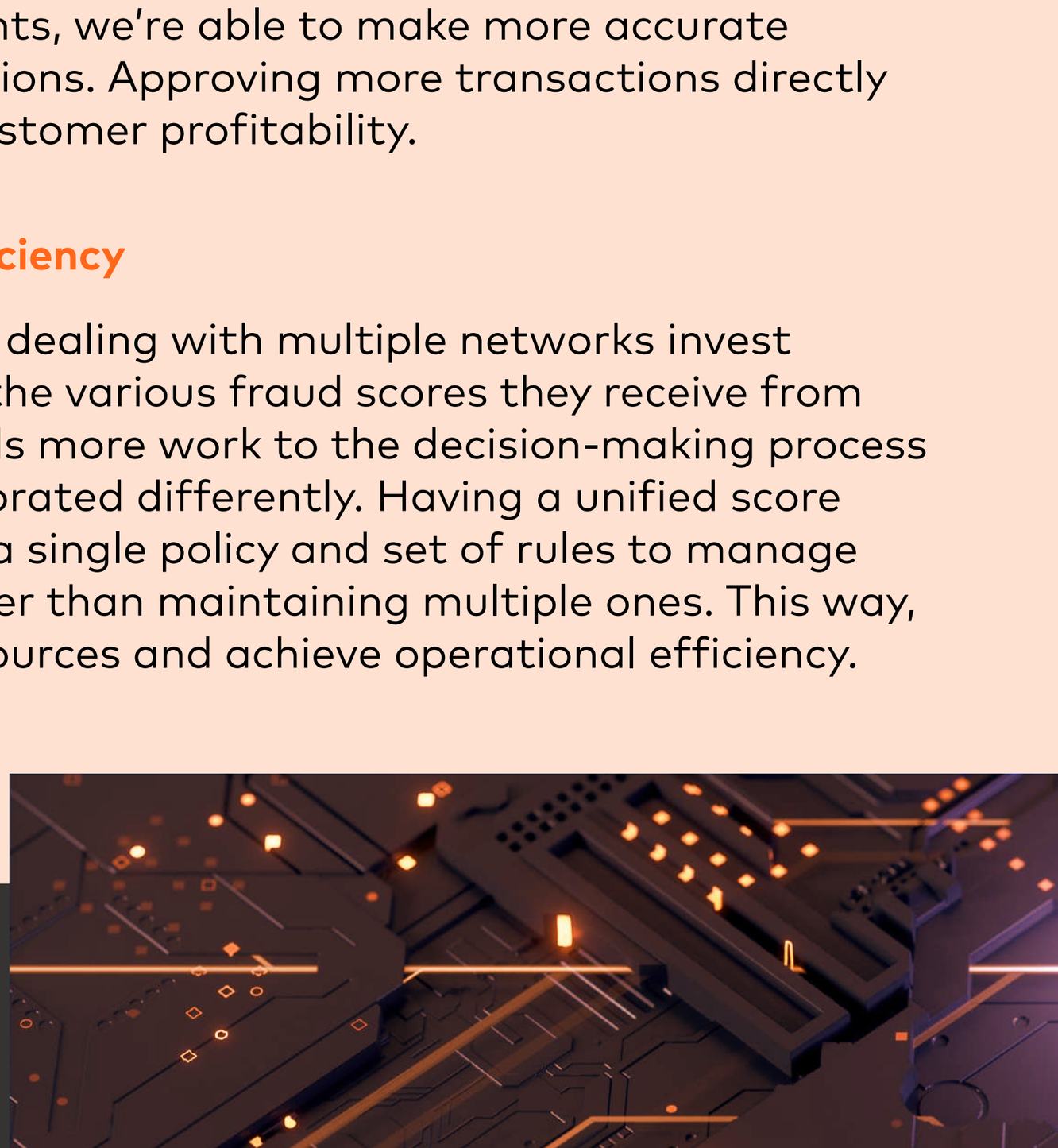


Increasing operational efficiency

Payment service providers dealing with multiple networks invest resources into navigating the various fraud scores they receive from different vendors. This adds more work to the decision-making process because all scores are calibrated differently. Having a unified score allows customers to have a single policy and set of rules to manage their entire portfolios rather than maintaining multiple ones. This way, customers can free up resources and achieve operational efficiency.

Uncover collaborative AI's potential with Mastercard Access

With Mastercard Access, we provide customers with the real-time infrastructure they need to deliver the additional insights necessary to thrive in today's fraud landscape, increase profits and provide an optimal customer experience. Grounded in trust, we're extending this same value-based approach to all industry players, regardless of brand, rail or payment type, to take advantage of collaborative AI and protect consumers' data privacy.



Seamless and secure: Embracing account-to-account payments with Mastercard Access

Jonathan Anastasia
Executive Vice President,
Crypto and Security Innovation

In recent years, consumers have embraced popular digital payment methods like Apple Pay and Google Pay and continue to adopt a variety of new and innovative payment channels. For one, account-to-account (A2A) payments are emerging as a direct and efficient solution, allowing money to move seamlessly between bank accounts.

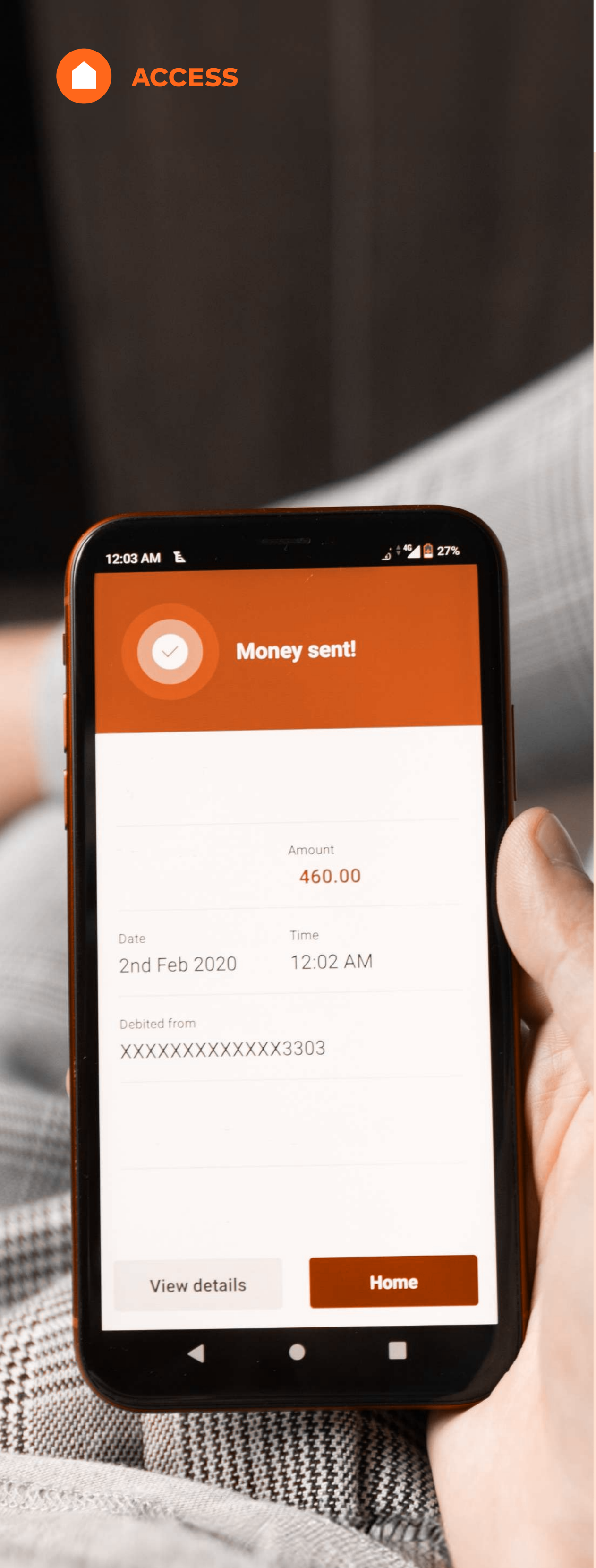
As technological innovation redefines digital payments, the Global Anti-Scam Alliance (GASA) predicts a 13% compound annual growth rate (CAGR) jump in A2A payments through 2026.[5] However, this progress comes with potential threats, particularly regarding security. As cybercriminals target digital payment options, it has become crucial for payments industry players to manage and mitigate these evolving risks to facilitate the growth of A2A and real-time payments (RTP).

Here we will explore how the payments industry can safeguard innovative digital payment methods like A2A against old and new scams. We'll also delve into how organizations can collaborate with Mastercard to establish a comprehensive services network to address a spectrum of scam risk solutions and fortify digital ecosystems, enhancing profitability and customer experiences.

Consumer financial losses from scams have exceeded

$1 trillion

according to the GASA Global State of Scams 2023 Report[6]



Shielding digital transactions against payment risks

The GASA Global State of Scams 2023 Report[6] reveals that consumer financial losses from scams have exceeded $1 trillion. Despite the continued rise of scams impacting individuals and organizations globally, innovative solutions are on the horizon.

As with all forms of digital payments, A2A payments come with their own security risks. Mastercard, in its blog post on A2A payment trends, risks and fraud solutions,[7] describes these risks, including social engineering attacks, authorized push payments and account takeover (ATO). One example of a prevalent social engineering attack we see is called a romance scam. These scams prey on consumers' vulnerabilities, developing false emotional relationships until the victim ultimately sends money.

We are also seeing fraudsters leverage deepfake artificial intelligence to mimic the voices of consumers' friends, family members and colleagues to gain the trust of targets and entice them to send money. Since peer-to-peer (P2P) payments are essentially equivalent to handing someone cash, senders and their banks often can't trace the malicious actor (recipient), who may have already deleted the account once the funds were transferred.

To defend against these threats and facilitate the growth of A2A payments, organizations can partner with a vendor that provides value-added services for scam risk solutions that cover the entire spectrum of digital payment methods.

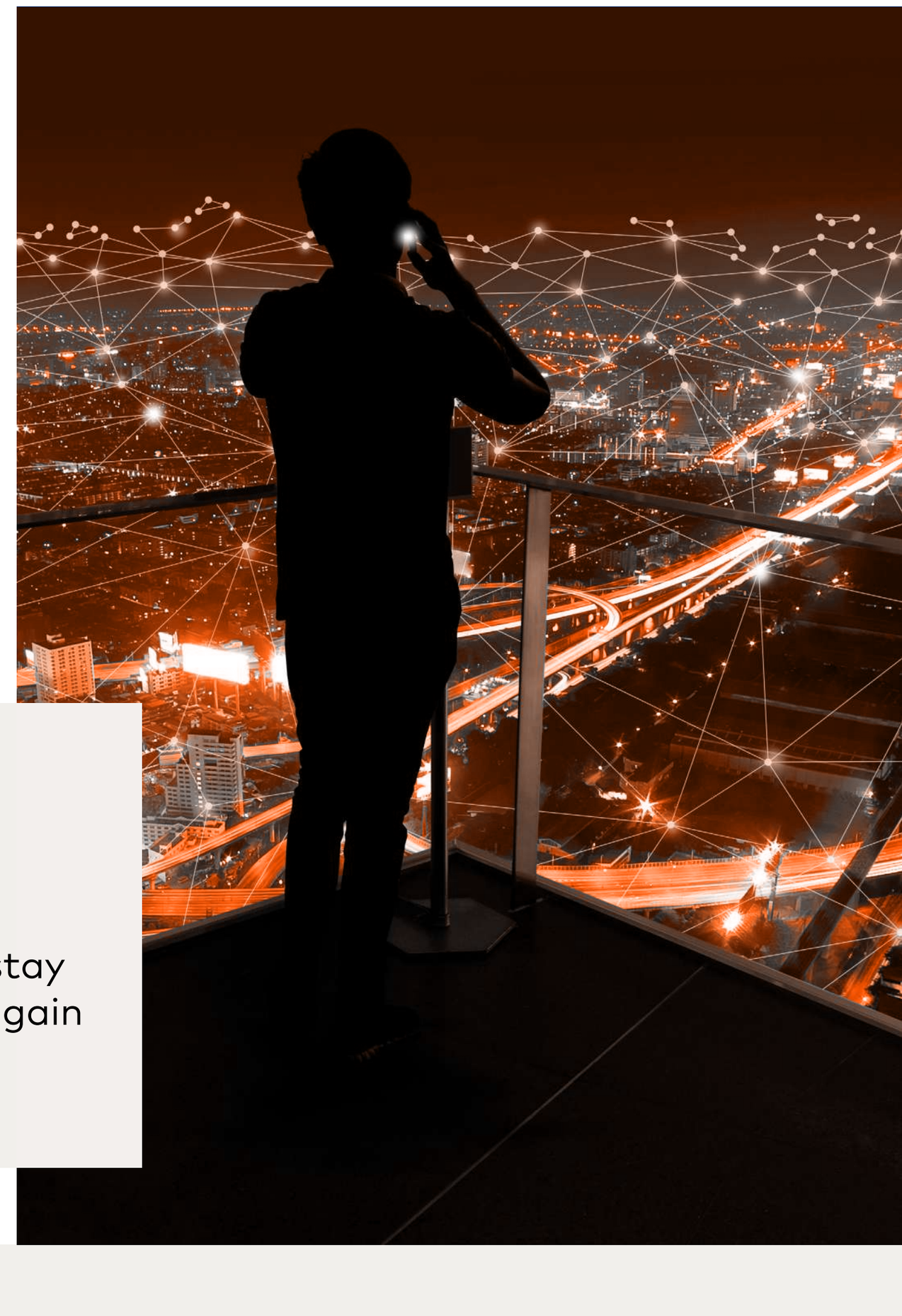
Customers are now able to subscribe to Mastercard's advanced AI-driven tools to combat fraud and identity scams across A2A, RTP and beyond, all via Mastercard Access. By leveraging this single point of connection, payments industry players can extend beyond card transactions, tapping into the growth potential of A2A and RTP service while also using these powerful tools to protect transactions from fraud.

New potential for fighting payments industry scams

One notable example of this is Mastercard's Consumer Fraud Risk (CFR) solution in the U.K., utilizing AI to enhance fraud and scam detection rates in A2A payments, preventing threats like investment and romance scams at the pre-transaction phase. This proactive approach has significantly reduced false positives, demonstrating the efficacy of fighting financial threats. Customers in the U.K. have reported that the use of CFR has significantly lowered their false positives, in some cases even down 5-to-1.

Recognizing the necessity for orchestration in scam risk solutions, Mastercard Access has built an infrastructure that facilitates seamless data flow between various cybersecurity and data intelligence solutions. Additional value-added services can be combined to provide a consistent consumer experience and enable growth beyond cards.

Mastercard Access provides customers with a unified profile for all their scam risk solutions, including identity and access management (IAM), case management and transaction monitoring tools. This orchestration provides customers with aggregated or disaggregated scores, allowing for flexible integration into existing fraud detection systems. By avoiding the need to replace current systems, Mastercard Access enables customers to access necessary scores and prevent disruptions to operations when it comes to the implementation of services.



With its streamlined tool orchestration, unified fraud scores and effortless implementation, Mastercard Access empowers payments industry players to stay ahead of fraud, preserve financial assets, gain customer trust and drive business results.

How Mastercard is leading the next generation of scam risk solutions

For payments industry players today, fighting fraud at the source means having the capabilities to orchestrate third-party data into their network of anti-scam solutions.

Research from the Federal Trade Commission underscores the growing impact of scams originating on social media networks, causing financial impact to 25% of consumers since 2021.[8] Because many scams begin on social media and telecommunications platforms, it is crucial that payments industry players tap into a services network equipped with scam risk solutions that analyze and orchestrate third-party data.

With Mastercard Access, customers can meet and exceed consumer expectations and drive profitability by offering a range of digital payment options, from transactions across card networks to other forms of payment like A2A. Mastercard is your trusted partner in navigating the future of digital payments, providing a secure and comprehensive solution for the evolving landscape of financial transactions.

ACCESS

Delivering a curated services journey with ubiquity and trust in every interaction

Haritha Nannapaneni
Senior Vice President,
Access Solutions

As the world has gone digital, the global payments ecosystem has evolved dramatically. Yet some aspects of payments rely on legacy infrastructure, essentially linear transaction flows between acquirers, issuers and card networks.

This infrastructure is challenged by the pace of real-time information sharing that's required to keep payments safe, secure and seamless. It is also challenged by other profound shifts in the payments landscape. Take, for example, today's heightened fraud risks, evolving regulatory context and compliance challenges, not to mention the resultant increase in operating costs.

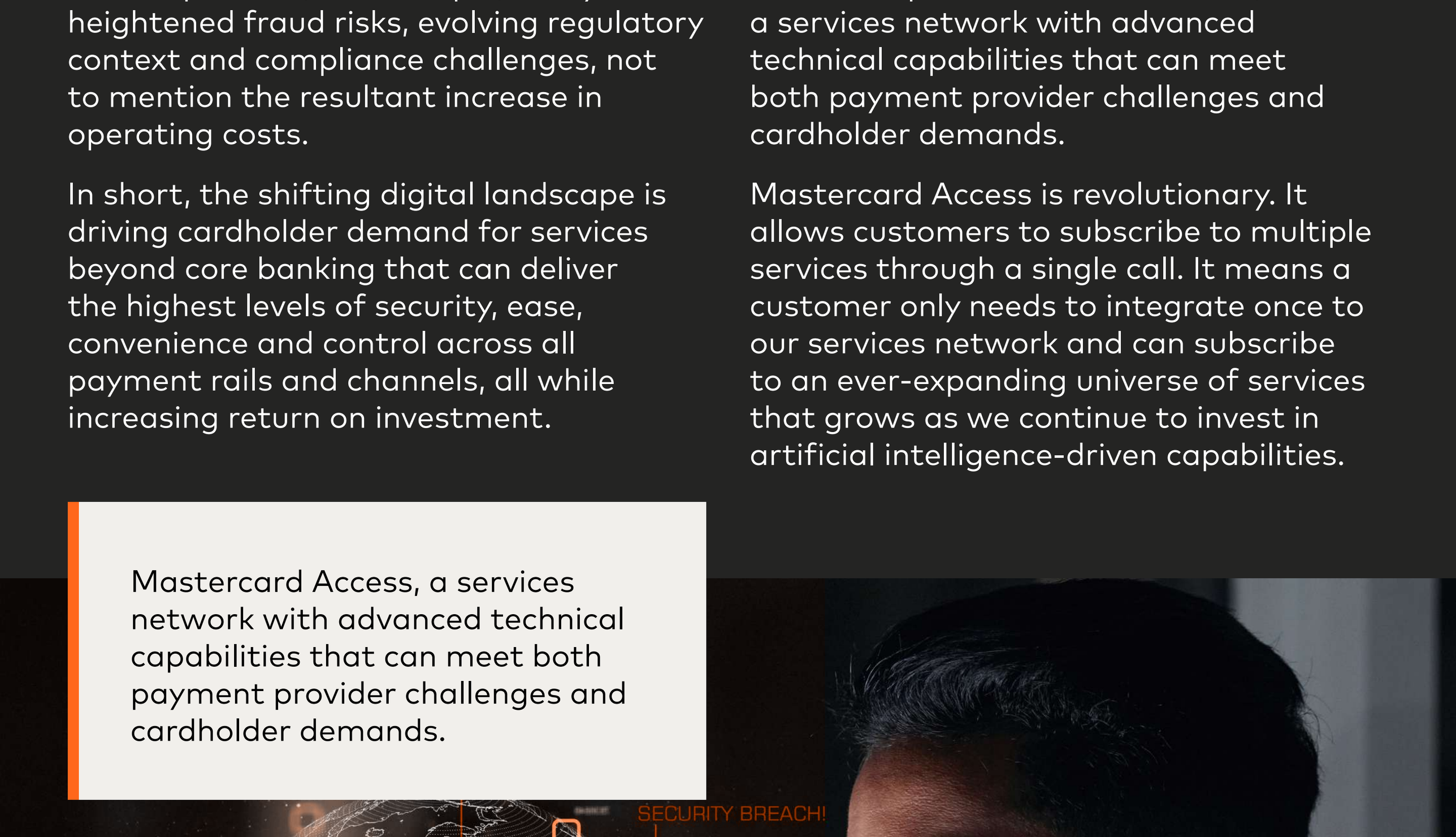
In short, the shifting digital landscape is driving cardholder demand for services beyond core banking that can deliver the highest levels of security, ease, convenience and control across all payment rails and channels, all while increasing return on investment.

Traditionally, to make such services work, payment participants needed to develop complex integrations with individual third-party services. This tended to slow things down, leading to drawn-out development cycles and compliance risks. Today's evolved ecosystem, on the other hand, requires value-added services to help drive competitiveness, growth and differentiation.

That's why, as a trusted technology partner to our customers, Mastercard has developed Mastercard Access, a services network with advanced technical capabilities that can meet both payment provider challenges and cardholder demands.

Mastercard Access is revolutionary. It allows customers to subscribe to multiple services through a single call. It means a customer only needs to integrate once to our services network and can subscribe to an ever-expanding universe of services that grows as we continue to invest in artificial intelligence-driven capabilities.

Mastercard Access, a services network with advanced technical capabilities that can meet both payment provider challenges and cardholder demands.



Mastercard Access is revolutionary. It allows customers to subscribe to multiple services through a single call.

What does Mastercard Access enable?

- **Built on advanced orchestration capabilities and built-in intelligence**, customers can subscribe to an expanding ecosystem of value-added services off the back of a single integration. Mastercard Access helps determine the sequencing of the services to be performed and the prioritization of service results. Further, simplifying integration to the services network, customers can leverage their existing Mastercard message formats (ISO message) or connect to the public cloud via API request to activate multiple services.
- **A curated experience** that helps customers of all types from processors and fintechs to issuers and everyone in between drive outcomes based on the role they play in the payments ecosystem. Mastercard also enables true connected intelligence by facilitating data connections to ancillary services like fraud reporting and model building. This extends Mastercard's rich services offering to customers on its payments network across all rails.
- **A secure, compliant and fraud-resistant experience** by replacing a fragmented set of service connections with a single trusted connection, Mastercard Access solves the structural problems posed by the increasing demand for services.
- **Boosted efficiency and timesaving** by leveraging Mastercard's trusted and reputable Privacy by Design service network. Mastercard Access also reduces payment participant time and minimizes resources dedicated to vetting every service they integrate for safety and resilience against fraud. This is enabled by Mastercard Access incorporating multiple embedded layers of privacy and security safeguards including data minimization, tokenization, encryption and anonymization.
- **A robust and trusted approach to regulatory compliance** as Mastercard partners with external organizations to understand existing and evolving regulations as well as market conditions.

What's simple and reliable is good for business

A significant number of customers are already connected to Mastercard's services network, realizing the benefits of subscribing to multiple value-added services through a single trusted connection. These benefits include reduced fraud rates, increased approval rates and improved cardholder digital experience to name a few.

Mastercard Access: Elevating customer experience across Europe through innovation

Mark Barnett
President, Mastercard Europe

Mastercard Access: Redefining the customer experience

The European market is made up of more than 40 countries and territories, each with its own unique profile. Despite this, European nations face the same challenges as those in other regions of the world; they need to continuously redefine their payments strategy, adapt to innovative new products, support government payment initiatives and implement major transformation programs. That's where Mastercard Access, Mastercard's single trusted connection to a services network, comes in. It is poised to help customers by providing them with the keys to a host of unrivaled payment and security innovations.

While Mastercard Access may seem like a new solution, over 100 banks and other payments industry participants across the world already benefit from its simplicity and value across their organizations with early adopters in Sweden, Israel, Italy and more.

As Mastercard's core competency for technology solutions provides a safe and secure network, the initial launch of Mastercard Access has connected early adopters to technology solutions designed to mitigate fraud and risk, and artificial intelligence-enhanced services that boost the transaction experience.

The roadmap for future services via Mastercard Access is inspiring because the possibilities are endless. And while there is more innovation to come in the future, current customers have already experienced the benefits that Mastercard Access can bring them, particularly those seeking sophisticated solutions tailored to their unique needs.

Take the example of one early adopter, Swedbank — a prime example of how European customers are enjoying the benefits Mastercard Access offers. They have praised the simplicity of using solutions on and off the Mastercard network, the easy integration with existing platforms and the ability to leverage global AI-driven insights to create internal efficiencies, reducing costs and fraud:

> "[The tools available via] Mastercard Access [were indispensable] in combination with our internal fraud prevention and fraud orchestration [layers], leveraging global Mastercard AI-driven insights to jointly go above and beyond what we had been able to do previously."
>
> – Swedbank

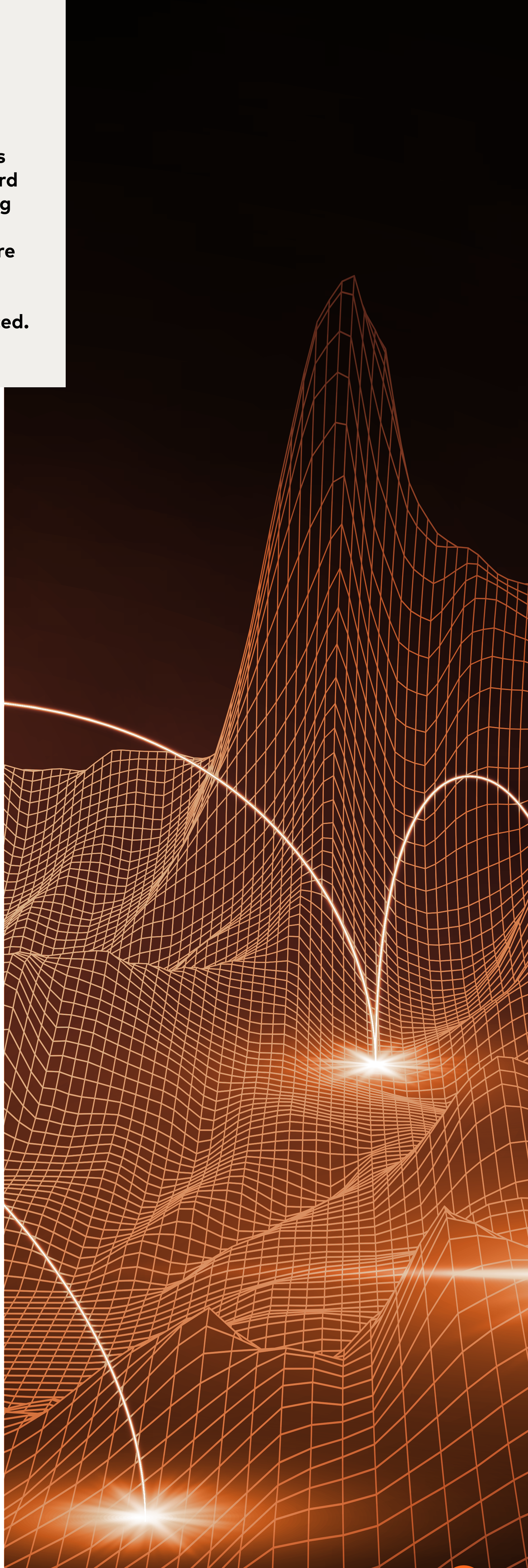
And Swedbank isn't alone. Customers have revealed how, prior to Mastercard Access, they were creating, developing and sourcing solutions for a disconnected ecosystem. Now they are relieved to see their need for multiple services or solutions across different networks and rails significantly reduced.

More equals more: Transactions, data and understanding

Mastercard's customers enjoy improved results and a more consistent cardholder experience by utilizing a broader range of services available through Mastercard Access. By layering solutions for transactions on and off the Mastercard Network and across the transaction lifecycle, the level of protection, especially against fraud, becomes substantial. Solutions like Transaction Fraud Monitoring and Decision Intelligence play a pivotal role in enhancing security and ensuring a seamless experience for cardholders. These innovative tools proactively monitor transactions, providing real-time insights and decision-making capabilities, thus significantly bolstering the overall security and reliability of the cardholder experience.

The trust factor

Our proven record as a provider of advanced technology is a key factor that distinguishes us among technology providers. Customers who join the Mastercard Access services network do so because of the trust they place in the Mastercard brand and its enduring reputation. Through Mastercard Access, they benefit from new synergies that help them navigate the complexities of the modern financial landscape.



CYBER

19 Deep currents: What you need to know on managing supply chain risk in 2024 →

22 Why chargebacks are changing →

26 The nature of fraud in fiat and crypto currencies →

Deep currents: What you need to know on managing supply chain risk in 2024

Security leaders know all too well the rapid growth of third-party cyber risk and its subsequent management challenges.

Rigo Van den Broeck
Executive Vice President, Cyber Security Product Innovation, Cyber and Intelligence Solutions (CAI)

In today's ever-changing digital world, the cyber risk landscape has become increasingly complex and filled with intricate supply chain layers extending beyond third parties.

In our latest edition of research on multiparty cyber incidents, "Ripples Across the ATTACK Surface," RiskRecon by Mastercard and Cyentia Institute collaborated on a study that dives into the current state of supply chain risk management. By assessing nearly 900 historical multiparty breaches, we identified the top tactics of cybercriminals, as laid out by MITRE ATT&CKs, and pulled other safeguarding insights to help ensure organizations don't get caught in the wake of a supply chain cyberattack.

Increasing depths

Ripple events have become more common as businesses evolve and adapt to keep up, weaving complex digital interdependencies to facilitate better business.

Multiparty incidents have increased at an average rate of **20% per year** over the last decade.

Based on our previous analyses, multiparty incidents have increased at an average rate of 20% per year over the last decade.

Challenge

Recent multiparty breach events have had serious, far-reaching consequences that demonstrate how cyber risk can originate in supply chain layers beyond immediate third parties. In fact, 65% of an organization's assets sit on infrastructure owned by an external entity or supply chain vendor. However, organizations are less likely to know who those supply chain vendors are, let alone receive rights to audit or risk assess them directly — leaving an organization exposed to backdoor supply chain cyberattacks.

Making waves

Ripple events are particularly concerning because their impact can spread beyond the initial victim and have far-reaching consequences. One of the standout findings from examining roughly 900 breach events is that the ripple effect from these breaches generated downstream effects to nearly 6,000 other organizations.

Additionally, the median financial loss for multiparty events is $1.4 million, compared to $191,000 for a single-party incident — meaning that in addition to the reputation damage and disruption to the business or consumers, a multiparty security incident typically cost seven times more than single-party events.

Attack styles

The following attack styles were identified as being commonly used by cybercriminals:

System intrusions

System intrusions are the riskiest type of ripple events, surpassing all others in frequency, total financial losses and the number of third parties impacted.

Valid user targeting

Targeting valid user accounts and exploiting trusted third-party relationships are the most common initial access techniques leading to ripple events.

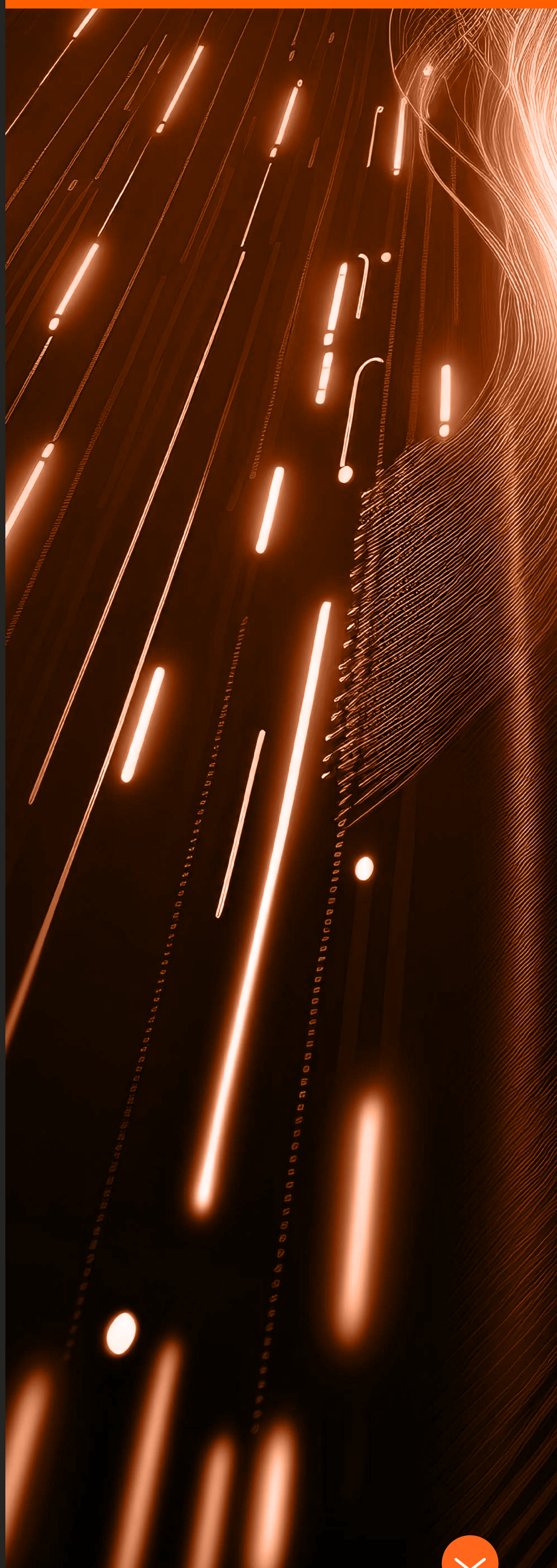
Public-facing application exploitation

Exploiting public-facing applications results in the largest proportion of financial losses from multiparty security incidents.

Malicious code injection

Malicious code injection and obfuscation were associated with 100% of reported financial losses and 87% of third parties impacted by multiparty security incidents.

Multiparty security incidents typically cost 7x more than single-party events.



How to stay protected

In an era where cyberattacks are becoming increasingly sophisticated and prevalent, a proactive approach to cybersecurity is essential.

At Mastercard, trust is our business. By using our advanced AI and extensive knowledge of payment transactions, we can examine the entire digital environment, including the supply chain, to identify weak spots. This evaluation stretches to fourth-party vendors, those companies that supply your known third-party vendors. Our customers will then have a comprehensive view of their supply chain risk and vulnerabilities, which will allow them to better understand their exposure to cyber risk and address critical issues quickly, protecting trust within their supply chain and with their customers.

Our evaluation process examines potential risk from all sources, which includes companies within the supply chain that might not be under direct monitoring by agencies. This thorough risk assessment process incorporates entities that may be overlooked by more traditional monitoring methods and provides businesses with a comprehensive assessment of risk, allowing them to proactively address potential harm from less obvious sources.

The final step in this process is to identify potential access points for attackers. We provide insights that help organizations identify the weakpoints that could be exploited. This insight empowers businesses to not just fix existing vulnerabilities but address areas that could be manipulated in the future.

To learn more about the findings from "Ripples Across the ATTACK Surface: Third Edition," download the report below:

Learn more

Why chargebacks are changing

Gaurav Mittal
Executive Vice President, Ethoca, Cyber and Intelligence (CAI)

Chargebacks have been around as long as credit card transactions. The goal was simple — to provide customers a fair way to get their money back in case something went wrong with their purchase, whether it was due to fraud or an unsatisfactory experience.

But the way we pay has changed from when chargebacks were first introduced — we could have never expected the meteoric rise of digital payments and the subsequent uptick in chargebacks. As we face the ever-evolving reality of digital payments, it's time to take stock of how chargebacks are changing and how businesses can ensure that they continue to provide consumer protection and experience while avoiding abuse of this important service.

The annual global chargeback volume is estimated to reach **337 million, a 42% increase from 2023**

Global chargeback volumes are rising

By 2026, the annual global chargeback volume is estimated to reach 337 million, a 42% increase from 2023. But expected chargeback growth varies across different regions of the world.

Europe's chargeback volume, for example, is projected to decline in coming years, driven down by the European Union's Strong Customer Authentication (SCA) rules intended to reduce card fraud. But while the rules have helped reduce fraud, merchants and consumers have, in turn, faced false declines and poor experiences at the point-of-purchase. Even with a slight decline from SCA, Europe will still need to manage an estimated $1.9 billion in chargeback volume in 2026.

The U.S. and Asia-Pacific regions, on the other hand, are positioned to see significant chargeback growth over that same period, with U.S. chargebacks expected to more than double from $7.2 billion in 2019 to $15.3 billion by 2026.

Regardless of region, issuers and merchants will need to continue finding ways to manage chargebacks and their bottom line. Businesses should implement tools offering reliable and secure payments intelligence through real-time collaboration networks. With better data sharing between merchants and issuers, these solutions can help prevent chargebacks, improve authorization rates, enhance consumer experiences and produce better outcomes for issuers, merchants and consumers.

> Mastercard is launching its First-Party Trust Program to help prevent first-party fraud and the burden it places on stakeholders while securing the payments ecosystem for all.

Not all chargebacks are due to 'true' fraud. As the way we pay has changed, the reasons for chargebacks have also evolved. Increasingly, chargebacks are the result of first-party fraud, which occurs when a cardholder makes a legitimate purchase but later claims it was fraud even though the goods or services were received.

This could be due to purchase confusion over unclear billing descriptors or the result of intentional misuse of the dispute process. But in both cases, the result is the same — a chargeback.

First-party fraud is a complex problem that requires a data-driven solution, with 75% of fraud experienced by digital businesses estimated to be the result of first-party fraud, according to Datos Insights.

Mastercard is launching its First-Party Trust Program to help prevent first-party fraud and the burden it places on stakeholders while securing the payments ecosystem for all. By using enhanced data to confirm the identity of the cardholder, Mastercard's First-Party Trust Program enables issuers and merchants to share information to help reduce cardholder confusion and more effectively spot instances of first-party fraud.

By making additional data elements available during both the pre-authorization and dispute stages, merchants and issuers can be more confident in spotting cases of first-party fraud, which can lead to better approval rates and remove more chargebacks from the ecosystem.

By 2026, the U.S. is projected to reach a value of **$12.9 billion in CNP fraud losses**

CNP fraud losses are also soaring

Consumer preference for digital interactions means we will likely continue to see high levels of card-not-present (CNP) transactions — especially in previously card-present heavy environments like grocery stores. CNP fraud losses will continue to impact businesses across the globe, although to varying degrees.

> Global CNP fraud losses are projected to reach a value of over $28 billion by 2026, representing a 40% increase from the $20 billion in global CNP losses expected in 2023.

The U.S. — which is projected to reach $12.8 billion in CNP fraud losses — is driving a large part of this expected growth, accounting for an estimated 40% of global CNP fraud losses by 2026.

Because merchants are liable for CNP fraud losses, it's incredibly important that they look for ways to tackle it — both genuine and first-party. Regardless of the region, businesses should pay attention to their CNP fraud, employing a multilayered approach that can resolve fraud, disputes and chargebacks at every touch point.

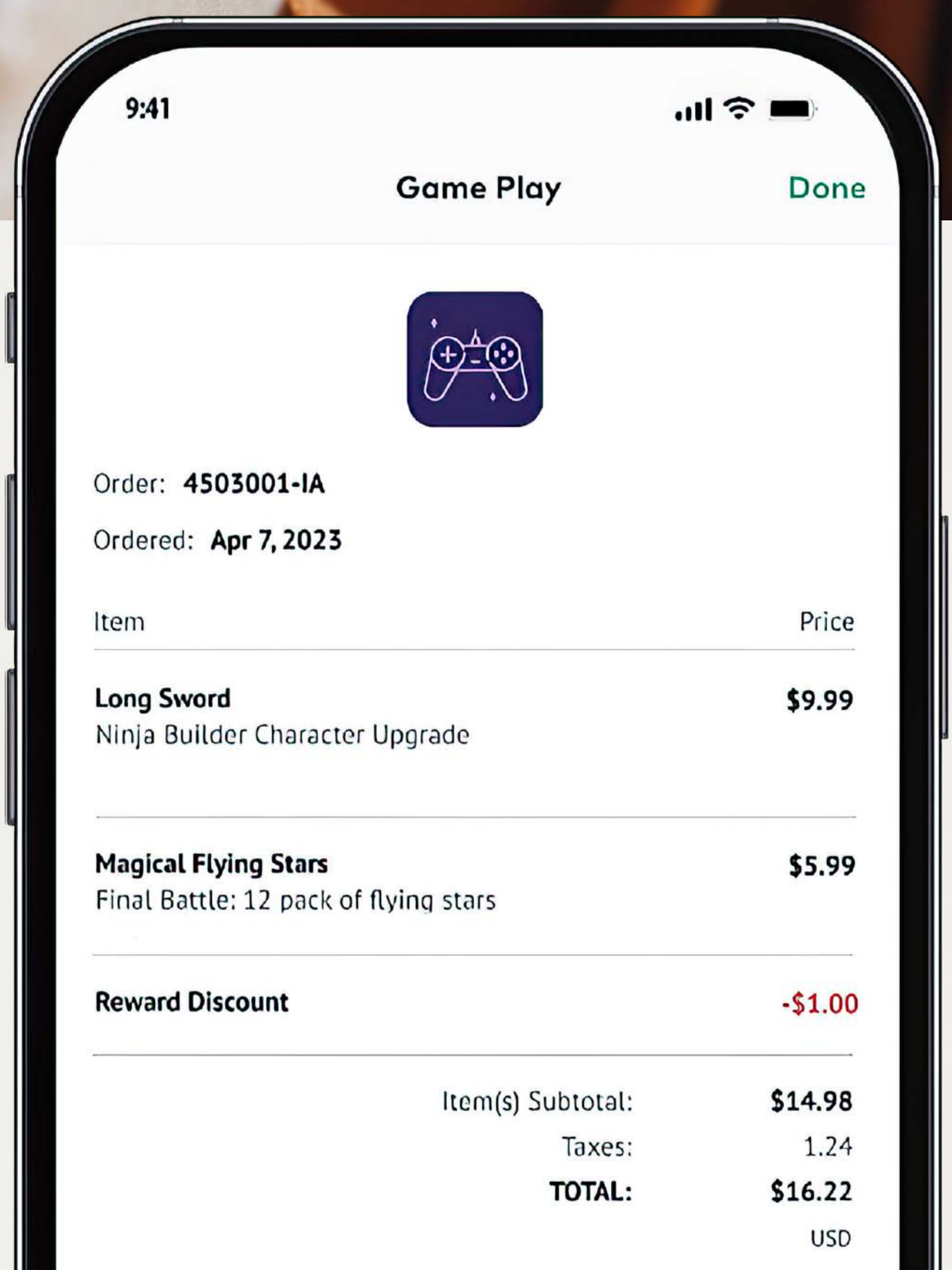
Stopping chargebacks in their tracks

Global chargebacks data suggests that the use of authentication and other chargeback prevention solutions are making a difference in stemming the tide of chargebacks. Better authentication can help lead to reduced cases of fraudulent purchases and their related chargebacks.

But increasingly, chargebacks are also the result of first-party fraud, due to cases of purchase confusion or intentional misuse. More and more issuers are investing in tools that bring clarity to cardholders about their purchases, helping to reduce cases of purchase confusion and helping back-office teams more accurately sort out legitimate transactions from fraud.

Whether providing more details directly to cardholders in their bank app or by giving call center agents access to more information, details like a clear merchant name, logo, fully itemized receipt and purchase history can help create a better customer experience while reducing cases of first-party fraud.

For issuers and merchants alike, managing chargebacks will require a multilayered approach to prevent disputes, no matter what's causing them. This requires greater collaboration between all stakeholders so we can share greater details like confirmed disputes or enhanced purchase details to better identify, resolve and deflect chargebacks.



The nature of fraud in fiat and crypto currencies

Addressing misconceptions that exist in the cryptocurrency debate

Jonathan Anastasia
Executive Vice President, Crypto and Security Innovation

Fraud is any activity that relies on deception to achieve a gain.[9] When we hear about crypto fraud, or, more broadly, virtual asset fraud, we typically think of deceptive practices to gain from some type of virtual asset activity. We immediately think that the "crypto" part of that phrase is the vulnerability, but that's rarely the case.

Fiat, not crypto, still appears to be the primary choice of financial criminals

Despite widespread fears that crypto is used for criminal purposes, fiat, not crypto, still appears to be the favored choice of financial criminals. The U.S. Treasury, in its 2022 National Money Laundering Risk Assessment,[10] highlights how fiat and traditional financial activities continue to be substantially more common than virtual asset use to perpetrate illicit activities. Similarly, Europol's 2021 Spotlight, 'Cryptocurrencies: Tracing the evolution of criminal finances,' states, "The overall number and value of cryptocurrency transactions related to criminal activities still represents only a limited share of the criminal economy when compared to cash and other forms of transactions."[11]

Where is the real fraud: crypto or fiat? Is the fraud origin nonfinancial?

Just because something is called a crypto scam or crypto fraud does not necessarily mean that it is unique to crypto activity or that it even touches cryptocurrency in some way. Crypto fraud must involve some "on-chain movement" transactions on the blockchain. Any fraud occurrence that ends with stolen crypto or a crypto scam but originates from nonfinancial activity or fiat activity still has an element of traditional fraud to it. If a criminal uses cloned credit cards to purchase crypto, that's credit card fraud, not crypto fraud. In this case, crypto just happens to be the asset stolen by the fraudster. Since this isn't crypto fraud, the traditional AML or transaction monitoring system at the bank or card company should pick up on the red flags for those credit card purchases.

Another common example is when a perpetrator acquires someone's private key to gain access to and steal their bitcoin. On the surface, we may say that that is crypto fraud or virtual asset fraud.

But the terminology changes when we consider the origin point. The perpetrator likely did not get the private keys from a crypto transaction flaw or hack into the blockchain. Rather, they probably manipulated the victim into giving up their private key or the victim was careless with safekeeping of their information, such as via a phishing attempt or a SIM swap.

The goal of the crime was to obtain access to the funds and is not specific to crypto, as it only involves crypto as an asset being stolen.

Use of virtual assets in scams and the actual root causes

The Federal Trade Commission[12] highlighted that from January 2021 to March 2022, more than 46,000 people reported losing over a total of $1 billion in crypto to scams.[13] The top cryptocurrencies used to pay scammers were bitcoin (70%), tether (10%) and ether (9%). Let's examine a few common schemes and their root causes:

Fraudulent investment schemes (i.e., Ponzi schemes, fake applications,[14] etc.) had $575 million in reported crypto losses during the January 2021 to March 2022 period.[15]

Description: Scammers introduce themselves as "cryptocurrency investment managers" and claim to have made millions investing in cryptocurrency. They may encourage their victims to invest in "cryptocurrency investment funds" via fake websites, showing great (fake) investment growth, only for victims to realize the funds are fake after they lose their money. Fraudsters may also convince their victims to download fraudulent mobile apps that have scammed millions from their victims, or they may use fake celebrity endorsements via hacked social media accounts to persuade victims to send an upfront fee in cryptocurrency which is never returned.

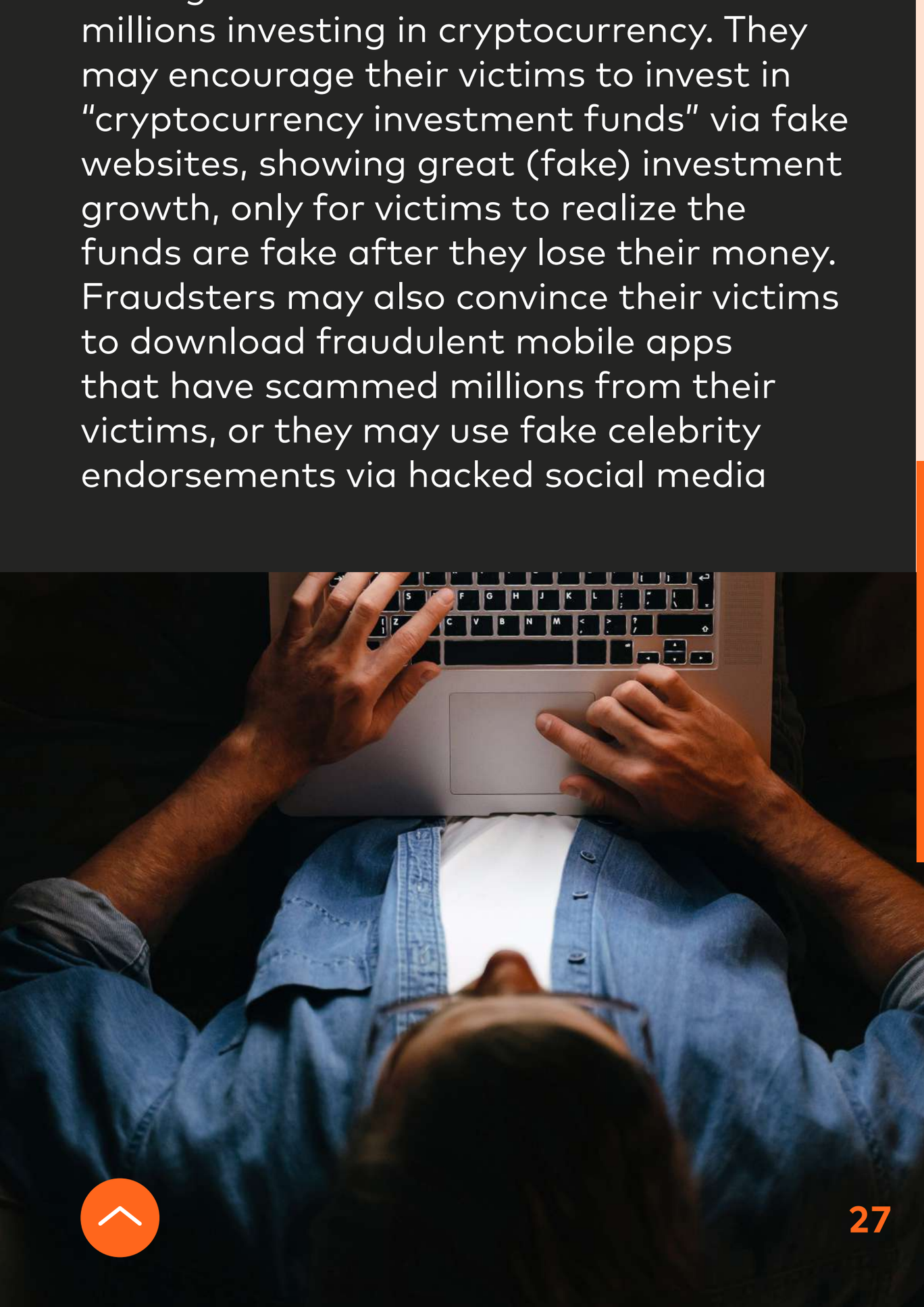
Root cause: For those victims who don't own crypto, the fraud starts before the crypto activity. The funds sent to the scammers are in fiat and utilize traditional payment rails, like wire transfer or electronic funds transfer. The scammers never convert the fiat into crypto. Instead, they persuade their investors into believing there is growth on their "account" by faking numbers on a fake website, fake social media or through some other type of communication.

Crypto romance scams with $185 million in reported crypto losses during the period of January 2021 to March 2022.[16]

Description: These scams occur when a criminal adopts a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim.[17] The FBI has also warned of a rising trend in which online romance scammers are defrauding victims by persuading them to send money to allegedly invest or trade cryptocurrency by directing their victims to fraudulent websites, applications or exchanges.

Root cause: The fraud occurred way before the crypto activity with the building of an online, nonfinancial, unverified relationship.

The Federal Trade Commission highlighted that from January 2021 to March 2022, more than 46,000 people reported losing over a total of $1 billion in crypto to scams.



In most romance scams, funds are typically moved in fiat, such as from a bank account or an ATM. If crypto is involved, funds are typically moved from fiat form, a bank account or an ATM, into a virtual asset service provider (VASP) of some sort to acquire crypto. There are multiple opportunities of possible intervention via the traditional fiat payment rails before there is a single bitcoin or other crypto transaction.

Credit card frauds with $28.6 billion lost worldwide to credit card fraud for the payments industry in 2020.[18]

Description: Credit card fraud occurs when someone that is not you uses your credit card or account information for an unauthorized charge. Some of the most common types of credit card fraud include:[19]

- **Card-not-present fraud:** Scammers use stolen credit cards to make online or by-phone purchases
- **Credit card application fraud:** Scammers use stolen personal information to apply for credit cards, which can remain undetected until the victim applies for a credit card or checks their credit score
- **Credit card skimming:** Skimmers are devices that steal credit card information from the magnetic strip on the back of the card, usually attached to credit card readers, ATMs, gas and retail stores, etc.
- **Lost or stolen credit cards:** Scammers steal someone's credit card, use a card someone has lost or intercept credit cards sent to cardholders in the mail

Root cause: The fraud has occurred way before any crypto activity. There are many opportunities for possible intervention via the traditional fiat payment rails (protection, detection, reporting) before there is any crypto transaction.

Decentralized Finance (DeFi) with the top 10 DeFi hacks for the period of January 2021 – June 2022 amounting in $2.4 billion.[20]

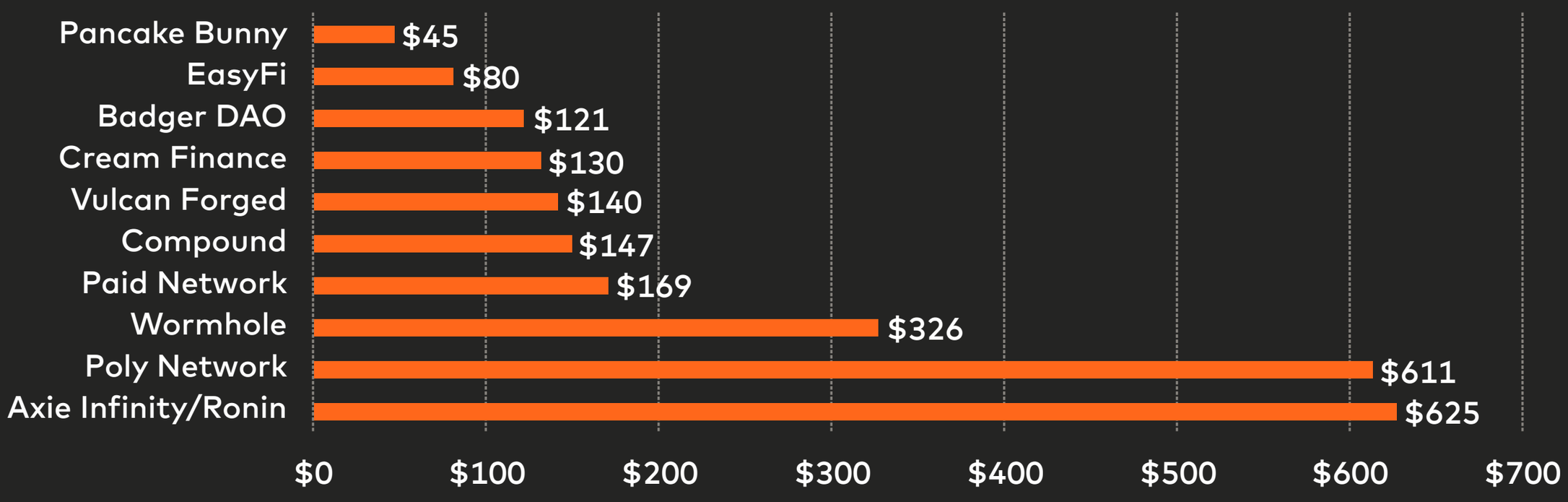
Description: These attacks were either an exploit of a system or in other cases were intentional fraudulent acts.

Root cause: These examples might be more closely correlated to virtual asset fraud, given these are not vulnerabilities in crypto assets, but rather risk management protocols within decentralized finance and decentralized applications. Further, phishing was the origin of several of these events.

$28.6 billion

lost worldwide to credit card fraud for the payment industry in 2020[10]

Graphic 1: Top 10 DeFi hacks ($M) 2021-2022



Source: CipherTrace cryptocurrency crime and anti-money laundering report, June 2022

Potential ways to combat the fiat fraud that eventually leads to crypto fraud

Fraud trends clearly call for increased efforts in training, education and AML and transaction monitoring intelligence to proactively identify and prevent continued attacks. The FBI recommends[21] financial institutions (among others) to:

- Proactively warn customers about such activity and provide steps for customers to report it.
- Inform customers as to whether the financial institution offers cryptocurrency investment services or other related services.
- Periodically conduct online searches for your company's name or logo to determine if they are associated with fraudulent or unauthorized activity.

The FBI recommends that investors remain vigilant, take the following precautions and look for the most common red flags:[22]

- Unsolicited requests to download investment applications.
- Promises for free money, large gains or extraordinary returns.
- Fake influencers or celebrity endorsements that seem out of place.
- Never share sensitive information with individuals with unverified identities.
- Never pay money to receive a prize or get hired when searching for a position.
- Avoid an unfamiliar exchange. Do your own research to ensure legitimacy.
- Use only encrypted websites when entering your debit or credit card details.
- Use hardware wallets, VPNs and strong passwords to protect digital wallets.

Conclusion

Financial fraud has been a longstanding issue in human history and continues to evolve. Despite the change in the means for executing scams — now involving the use of virtual assets — fraudsters will still rely on the same basic aspects of human psychology for success.

When it comes to crypto fraud, which by definition must involve on-chain activity, increased education, monitoring and insights will help both financial institutions and investors identify the scams emanating from fiat rails and mitigate risks before they take place.

IDENTITY

32 How online retailers can fight fraud during the sales season →

35 Preventing promo abuse: Online retailers' fastest growing risk →

39 Fighting first-party fraud to retain trust and avoid chargeback misuse →

How online retailers can fight fraud during the sales season

Ting Van Osdol
Senior Vice President,
Global Client Success, Identity

Mastercard SpendingPulse™ predicted this most recent holiday season would be a promising one for retailers, with up to 3.7% year-over-year[23] (YoY) growth anticipated in retail sales across the U.S. In addition, global data,[24] indicates that the holiday season (Nov. 1 – Dec. 31) will total $1.19 trillion worldwide, a 4% YoY online sales growth.

As we all get back to business post-holiday season and retailers calculate the success of their sales, one thing is certain each and every year: Fraud is ever present. According to the data[25] calculated at the close of last year's holiday season, the average number of suspected digital fraud attempts during Thanksgiving and Cyber Monday was 82% higher globally than during the rest of 2022 and 127% greater for transactions outside of the U.S.

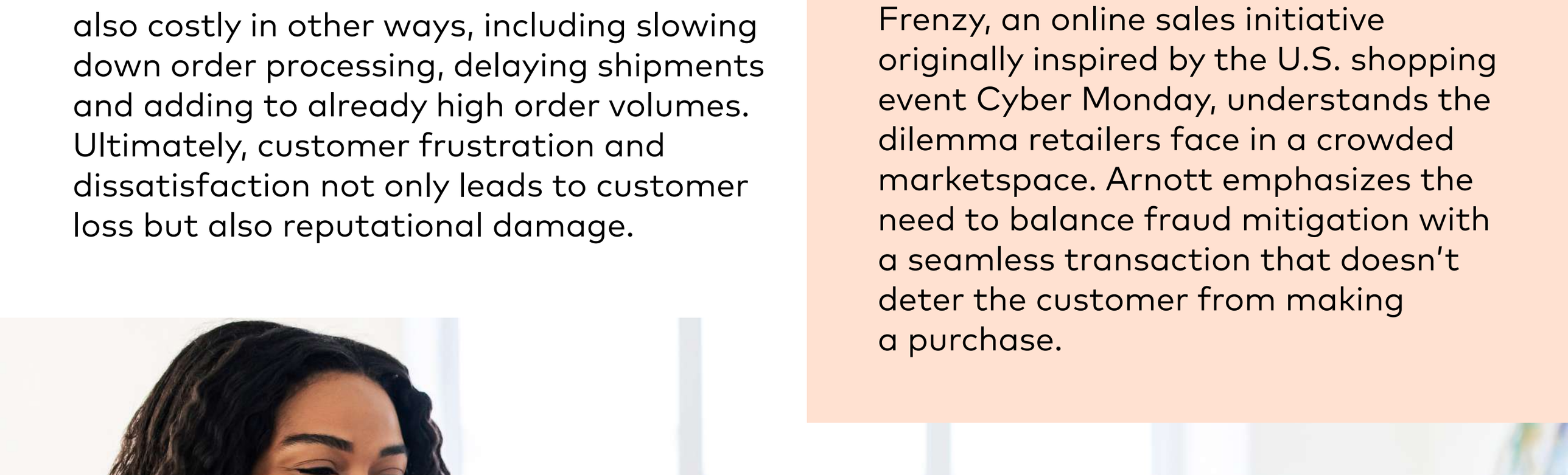
The impact of fraud on retailer profitability can be devastating. Specifically, research indicates that merchants are expected to lose up to $206 billion between 2021 and 2025.[26] Fraud is also costly in other ways, including slowing down order processing, delaying shipments and adding to already high order volumes. Ultimately, customer frustration and dissatisfaction not only leads to customer loss but also reputational damage.

FAQ

So how does your fraud team prepare for costly seasonal scams?

How do you fight fraud during the sales period without impacting your customer experience?

Mastercard client Grant Arnott, the cyber-sale pioneer behind Click Frenzy, an online sales initiative originally inspired by the U.S. shopping event Cyber Monday, understands the dilemma retailers face in a crowded marketspace. Arnott emphasizes the need to balance fraud mitigation with a seamless transaction that doesn't deter the customer from making a purchase.



Context matters

Every customer has unique preferences and varying levels of tolerance for friction, depending on the context of the purchase — its price, how quickly they need the item and more. Therefore, a one-size-fits-all approach to fraud prevention and friction doesn't work because it ignores the context behind each interaction and transaction.

While a customer may expect and accept a certain level of friction, merchants must be wary of relying too heavily on manual reviews. Our own research indicates that merchants who rely solely on manual fraud prevention techniques to combat fraud may soon find their losses from false declines outweigh any savings. For example, false positives for fraud cost merchants upwards of $450 billion in revenue — and, significantly, as much as 20% of rejected transactions are, in fact, legitimate.[27]

Strategic friction

It all comes down to strategic friction. Powered by behavioral biometrics, strategic friction enables businesses to introduce an appropriate level of friction during the customer journey according to their risk score. For example, if a customer's risk score is high, introducing step-up authentication measures before you allow them onto your platform makes sense. Alternatively, a customer with a low-risk score can enjoy a smoother, more seamless account sign-up and transaction.

If a customer's risk score is high, introducing step-up authentication measures before you allow them onto your platform makes sense.

Are you ready?

At Mastercard, we recommend a layered approach. This approach involves using a customizable, automated identity verification solution that collects and analyzes data from authoritative, global sources. These sources should prioritize diversity, efficiency and privacy, forming a robust foundation for the identity verification process.

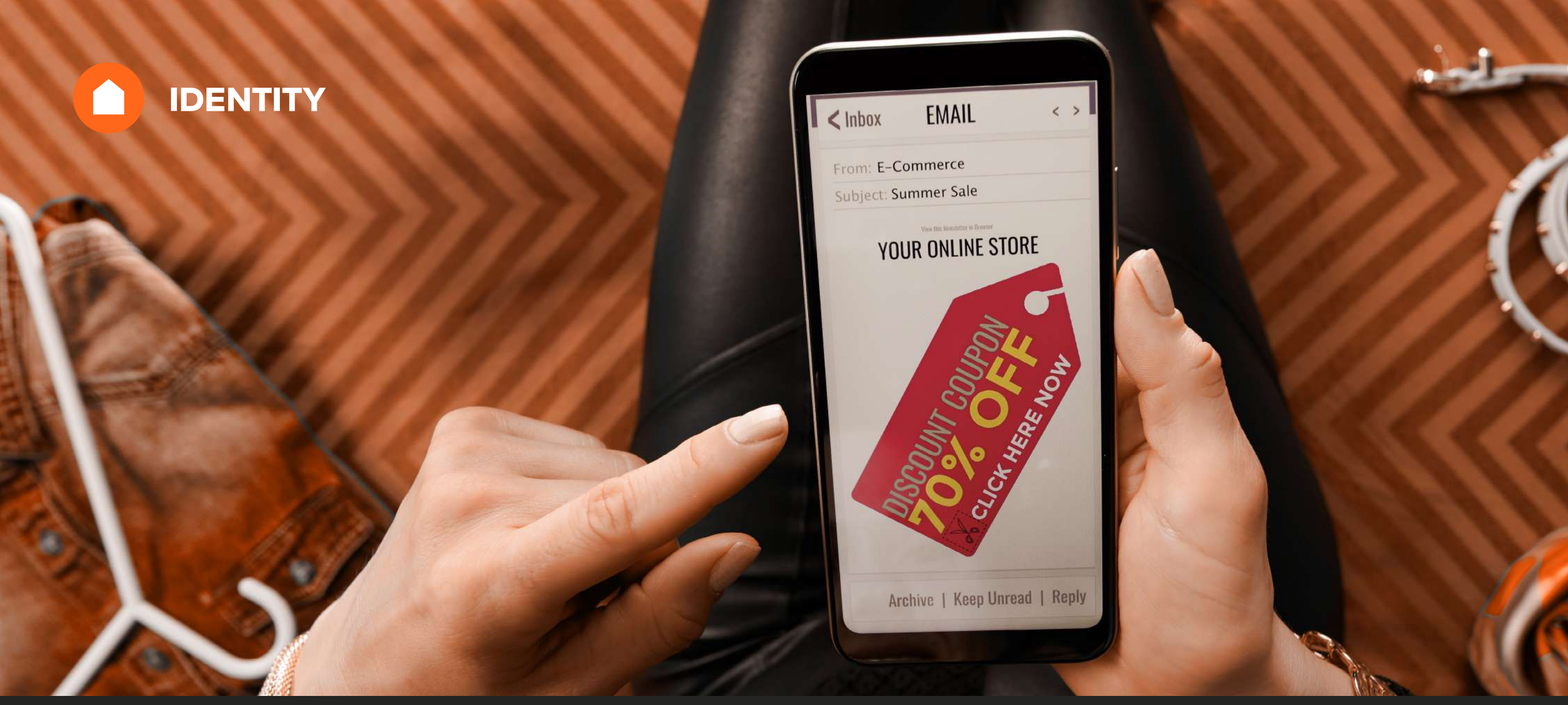
Before any transaction is authorized on your platform, your identity verification process must reliably assess the legitimacy of the customer according to their risk profile. This approach enables you to more confidently identify good customers up front, routing them through a fast approval process while rejecting fraudsters immediately. Moreover, this approach subjects only high-risk customers to in-depth reviews, thereby providing better support to your internal review team with actionable risk assessment information.

The Identity Engine

Mastercard's Identity Engine is a real-time customer identity verification solution that helps online retailers distinguish between good customers and bad actors. The Engine applies sophisticated data science and machine learning to validate a customer's identity elements and analyze their behavior in digital interactions.

The Identity Engine powers our account opening solution and manual review tool, Pro Insight. The former enables merchants to assess fraud risk before a customer even gets to the checkout stage. By categorizing customers into low-risk and high-risk buckets during account opening, sign-up flows are streamlined and fraudulent activity is minimized. This ensures all incentives offered are only provided to legitimate customers, thus growing your business.

Ting has spent the past nine years in Identity, working closely with customers and partners on leveraging identity verification data and insights to fight fraud and reduce customer friction. She runs the global client success team and for the past two years has been the acting GM of the Amsterdam office (formerly Ekata).



Preventing promo abuse: Online retailers' fastest growing risk

Micheal Pettibone
Senior Vice President, Global Strategy and Development, Identity

Promo codes can be a powerful tool for boosting engagement during peak sales season for merchants and online businesses, but they come with their own set of risks. As our partners at Ravelin[28] have reported, promotion abuse is the fastest growing fraud threat facing online retailers today, with more than half of companies noticing an increase in 2021.

Promo abuse, or promo fraud, occurs when promotional codes are used fraudulently or are not authorized. There are many ways this can be done, including:

Stacking or using multiple codes in a single transaction

Using automated tools to generate or duplicate codes and bypass restrictions

Reselling or trading codes

Exploiting loopholes to gain additional benefits, such as using an expired code or manipulating the usage limits

Sharing the codes publicly (on social media or dedicated coupon websites), allowing anyone access

The impact of promo code abuse

When promo codes are used in unauthorized ways, it impacts the revenue generated from sales, erodes profit margins and devalues the entire marketing campaign. This reduces profitability for the business engaging in a promotion. Merchants heavily rely on promotional campaigns to attract new customers, drive sales and increase brand awareness, particularly in a crowded market. When abuse occurs, it disrupts these strategies, making it challenging for businesses to accurately measure the effectiveness of their efforts.

Monetary loss is not the only impact. A more nuanced issue is how promo abuse can strain customer relationships. Customers who play by the rules and notice the exploitation of promo codes may feel unfairly treated. This dissatisfaction can lead to loss of trust and potential resentment among loyal customers.

Promo abuse also increases operational complexity. When marketing proposes a promotional campaign, they typically need approval from other departments. This involves presenting the success of past campaigns and the current campaign's objective. When fraud occurs, the data gets convoluted. It also requires resources and time to detect, investigate and address incidents of abuse. This time-consuming process diverts attention and resources from core business activities, ultimately increasing overhead costs.

In a recent example, a large fintech company had to shut down 4.5 million accounts last year upon discovering "bad actors" had hacked their incentive and rewards program. The fallout was significant, with revenue loss that not only negatively impacted business but also saw shares plummet.

How to detect promo abuse

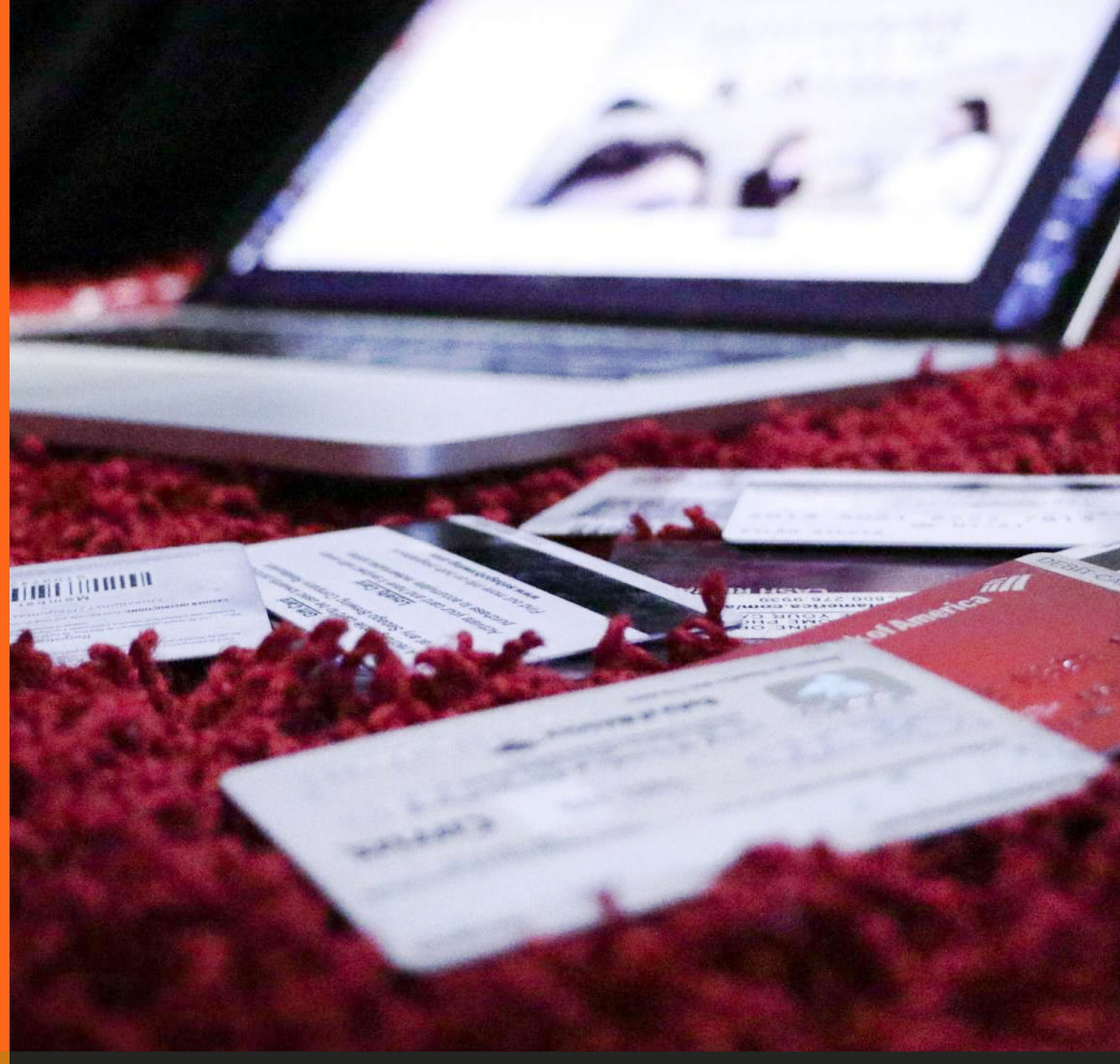
Fraudsters adopt various strategies to abuse promo codes, harming businesses across industries. Detecting fraud as it occurs can be challenging, often only becoming apparent when the damage is already done. Thankfully, there are best practices established to improve promo abuse detection.

Behavior analysis

Unusually high redemption rates by specific customers can often indicate abuse. When analyzing customer behavior associated with promo code usage, it's essential to look for patterns. Patterns of abuse can indicate if a customer is consistently using multiple codes, making large purchases with heavy discounts or exploiting loopholes in the code redemption process.

“

For high-value or high-risk promotions, it’s recommended to manually investigate transactions or customer accounts that raise suspicion.



Location analysis

Just like analyzing customer behavior, it’s recommended that fraud teams do a geographic and IP address analysis. Unusual patterns can indicate fraud, such as multiple redemptions from the same IP address or a concentration of redemptions from a specific location. It’s also important to monitor user accounts. If one user has multiple accounts or suspicious account creation patterns, this is a flag for potential abuse.

Machine learning

Another important detection tool is employing machine learning or statistical analysis techniques to identify anomalies in code usage data. Irregularities such as sudden spikes in redemptions or deviations from standard code usage patterns may point to abuse.

Third-party monitoring

It is worth the time to monitor social media or coupon websites to see if a promotion is shared in a way other than what is intended by the campaign. Specifically, merchants should monitor for instances of unauthorized sharing or distribution of codes that could lead to abuse.

Manual review

For high-value or high-risk promotions, it’s recommended to manually investigate transactions or customer accounts that raise suspicion. While doing these manual reviews, businesses should pay attention to customer complaints or reports related to promo codes. This way, a fraud team might discover abuse or misuse by actively addressing customer concerns about the promotion.

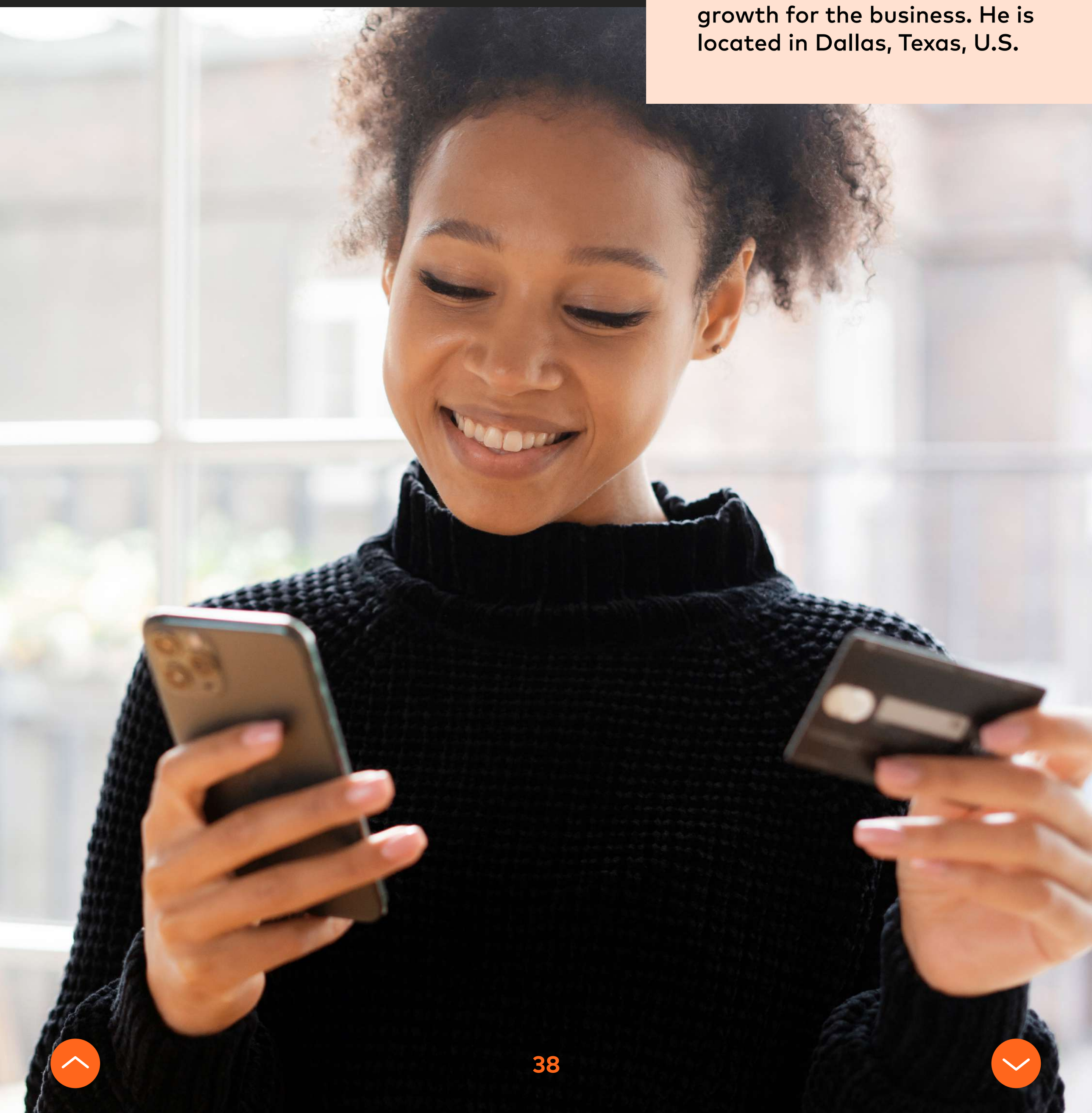
How to prevent promo code abuse

Because the most common form of promo abuse fraud is the creation of fictitious accounts, the ability to identify new accounts while weeding out fraudulent ones is important. Our account opening solution, powered by our Identity Engine, gives businesses access to the right data to quickly distinguish good customers from bad actors. Better still, because only limited inputs are required, businesses can maintain low-friction sign-up flows for customers who are eligible for a promotion.

To best detect and prevent promo abuse, businesses should invest in identity verification that leverages machine learning, dynamic risk signals and data analysis. This will not only streamline the account sign-up process for legitimate new customers, but also save fraud teams valuable time in manual review.

Due to a hacking of its incentives and rewards system, a fintech company recently shut down **4.5 million accounts**

Micheal is Senior Vice President, Strategy & Development, Identity at Mastercard leading global strategy, innovation and growth for the business. He is located in Dallas, Texas, U.S.



Fighting first-party fraud to retain trust and avoid chargeback misuse

Nili Klenoff
Senior Vice President, Product Innovation, Identity

Chargebacks are a protective measure intended to safeguard consumers' financial health. However, this can mean that merchants are at a disadvantage when it comes to disputing chargebacks. Unless retailers can provide strong evidence to dispute a customer's chargeback claim, they are likely going to incur the loss. The cost of chargebacks to the industry is so substantial that Mastercard has projected that the global chargeback volume will hit $111.47 billion by the end of 2023.[29] So it's never been more important for merchants to have best-in-class mitigation measures in place.

The costs and consequences of chargebacks

When calculating the true cost of chargebacks to merchants, there are both direct and indirect, hidden costs. The most immediate financial impact of a chargeback is the loss of revenue from the original transaction. However, as the Merchant Risk Council has calculated, the actual cost exceeds the directly disputed dollar amount. The total cost can be as much as 1.5 to 2.5 times higher once operational costs and payment processor or issuer fees are taken into account.

The status of the actual item adds to the chargeback cost too. If the product is returned to the merchant, they have to calculate the shipping, restocking and packing costs. However, if the product is not returned, the merchant loses both the payment and the product.

The cost of operations also plays a role. How much time and how many resources are spent managing a chargeback? It's not a straightforward process to compile a compelling case against a chargeback. If a merchant wants to dispute a charge, transaction evidence needs to be collected, on top of communication with the bank and processors.

Finally, there's the reputational impact to consider if a chargeback dispute leads to bad reviews. The consequences of brand damage can be far-reaching and costly.

The cost of operations also plays a role. How much time and how many resources are spent managing a chargeback? It's not a straightforward process to compile a compelling case against a chargeback.

Chargeback prevention tips for merchants

Merchants can take preventative measures that can effectively mitigate the risk of friendly fraud. This includes investing in staff training to better exercise effective dispute management and provide proactive customer communication. A merchant equipping their team with the tools necessary to deescalate a situation goes a long way, not only in preventing chargebacks but also enabling a better consumer experience.

However, when it comes to investing in technology, it's important to choose tools and products that enable true digital identity verification and risk assessment. When a merchant knows that a customer is who they say they are, they not only mitigate identity fraud but can also prevent friendly fraud and chargeback abuse.

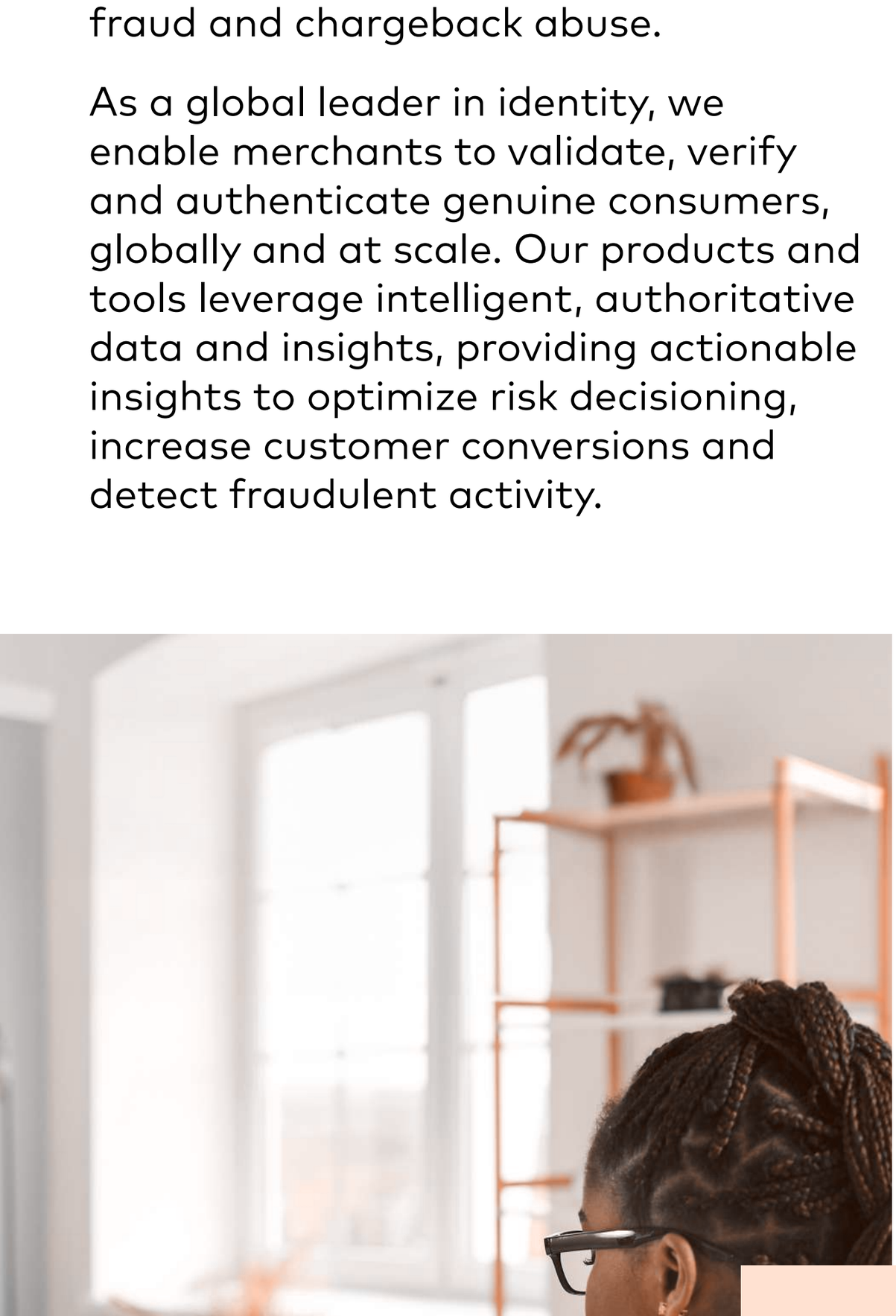
As a global leader in identity, we enable merchants to validate, verify and authenticate genuine consumers, globally and at scale. Our products and tools leverage intelligent, authoritative data and insights, providing actionable insights to optimize risk decisioning, increase customer conversions and detect fraudulent activity.

Mastercard targets friendly fraud to protect merchants

Mastercard is addressing the growing problem of chargeback abuse and first-party fraud with First-Party Trust. By leveraging data from at least two historical transactions that merchants provide, the First-Party Trust program allows issuers and merchants to better determine if a cardholder authorized a transaction that the cardholder is now disputing as fraudulent.

Importantly, if the merchant's data provides compelling evidence that the cardholder authorized the disputed transaction, the Mastercom system rejects the chargeback. Mastercom then provides the compelling evidence to the issuer.

Mastercard empowers merchants to navigate — and mitigate — evolving fraud trends.



Mastercard has projected that the global chargeback volume will hit

$111.47 billion

by the end of 2023

Nili is responsible for Mastercard's Authentication Network, including EMV 3DS, AI-powered risk detection capabilities and biometric authentication solutions to drive trust and security in digital commerce with a flawless cardholder experience.

RISK & RESILIENCY

42 AI can help banks sharpen payment resiliency and maintain consumer trust →

44 Transaction risk management technology secures the digital financial environment with Saudi Awwal Bank →

46 Navigating sophisticated transaction fraud trends in 2024 →

49 Sustainable cards for an environmentally conscious future →

51 Mastercard's RiskX: Navigating the future of cybersecurity and trust →

AI can help banks sharpen payment resiliency and maintain consumer trust

With millions of transactions taking place every day, any disruption to the processing of card payments by banks — even for a matter of minutes — could jeopardize consumer trust and confidence.

Laura Quevedo
Executive Vice President, Cyber & Intelligence, Payment Resiliency & Platform Advancement

At the same time, issuers are facing obstacles that can hinder this process. Cybersecurity threats have quadrupled in the last three years and cyberattacks are expected to cost companies $10.5 trillion annually worldwide.[1] An increasingly complex payment journey and greater regulatory requirements are also collectively giving rise to an enhanced need for resiliency. In fact, the impact of outages is prompting increased scrutiny from regulators who are interested in how financial institutions are building resiliency into their payment systems.

It's essential that issuers get the support they need to ensure card payments run seamlessly. To help banks address these challenges, Mastercard recently added three new capabilities to its suite of Payment Resiliency solutions.

Cyberattacks are expected to cost companies

$10.5 trillion

annually worldwide

RISK & RESILIENCY

Dynamic Decisioning employs AI technology to evaluate more than 200 dynamic variables that make an intelligent decision on behalf of the issuer, eliminating dependency on manual configurations and improving decision accuracy. The AI model leverages learnings from historical decisioning patterns, allowing it to imitate the issuer's decision had they been available.

Account Balance Listing allows issuers to share cardholder spend limits with Mastercard to mitigate overdraft and over-credit-limit concerns. The issuer defines account-level allowances, personalizing each authorization decision to the individual cardholder. Account Balance Listing also enables continuous monitoring of account level spend. As transactions are approved, the Account Balance Listing is updated with the modified allowed spending amount.

Contingency Manager enables issuers to create multiple sets of fully customized parameters that the authorization service will rely on during disruptions, whether predictable (such as a scheduled outage) or unpredictable (such as a cyberattack). By specifying in advance what configurations to use and when, banks ensure that cardholders can continue to transact during any type of disruption.

With an increased focus on resiliency, Mastercard is harnessing the latest AI technology to make it even easier for our customers to keep payments flowing. This improves consumer experience and protects trust across the ecosystem.

Transaction risk management technology secures the digital financial environment with Saudi Awwal Bank

Maria Parpou
Executive Vice President,
Mastercard Gateway

Sudhir Jha
Executive Vice President,
Brighterion, Cyber and
Intelligence Solutions (CAI)

Cyberthreats are a rapidly growing challenge in the payments industry. As cybercriminals get smarter, innovative partnerships can help proactively detect, prevent and mitigate fraudulent activities. Our partnership between Mastercard Gateway and Brighterion does just that, ensuring enhanced security for both acquiring customers and their enterprise merchants.

Our Gateway and Brighterion anti-fraud integration — Transaction Risk Management (TRM) — leverages Brighterion's artificial intelligence (AI) and machine learning to provide real-time analysis and enable acquirers to use advanced technology to better help and protect their merchants, reduce fraud and approve more legitimate transactions.

الأول
SAB

Recently, we announced a new partnership with Saudi Awwal Bank (SAB) in Saudi Arabia to offer consumers across the country greater access to secure digital transactions. Through this partnership, SAB will leverage Mastercard Gateway's advanced Transaction Risk Management technology to deliver safe and seamless digital transactions, customer protection from cybercrime and payment fraud prevention. Driven by cutting-edge data science, the Mastercard Gateway AI-powered technology helps to reduce financial risk by proactively assessing transactions for vulnerabilities.

Speaking of the partnership, Yasser Al-Barrak, chief corporate office and institutional banking officer at SAB, reinforced how this new collaboration secures the digital financial environment for their customers and is imperative as Saudi Arabia Vision 2030 draws closer.

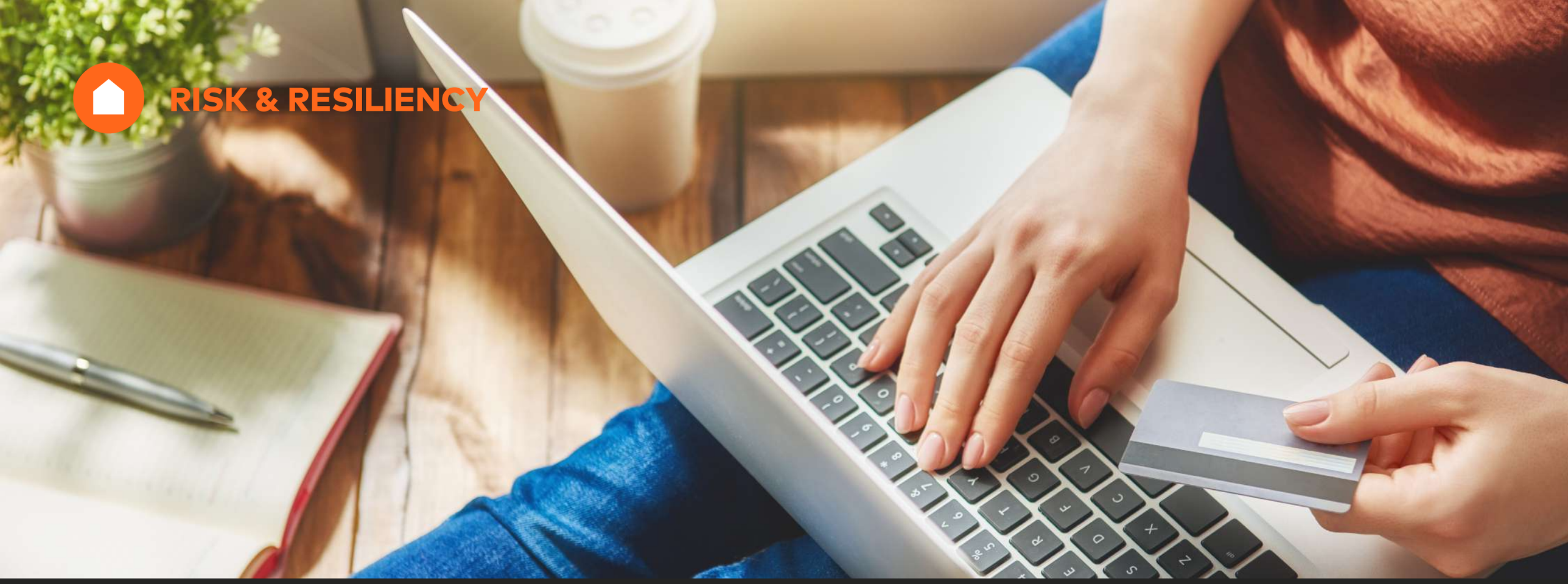
"As we evolve our digital proposition, we have chosen Mastercard, our long-standing, trusted partner, to support our efforts in the cybersecurity space. Mastercard is ideally positioned to help us boost our capabilities to mitigate financial risks and increase peace of mind," Al-Barrak said.

"This partnership reflects our commitment at SAB to provide a reliable and secure digital financial environment for all our customers. We continuously strive to equip them with advanced tools and solutions that instill confidence in conducting online banking transactions," he added.

At Mastercard Gateway, we see our role in creating this unified vision between customer behavioral patterns, security and payments as essential. Our support for SAB and other customers across the globe is part of Mastercard Gateway's evolution from a traditional gateway provider to commerce facilitator. In this role, Mastercard Gateway can orchestrate a dynamic offering providing seamless and secure payment experiences for merchants and their customers.

And while we thrive on keeping transactions safe at Mastercard, we don't just stop at technology. Beyond the collaboration, this new Transaction Risk Management technology integration highlights our belief that customer service and experience are equally important in the fight against fraud. We provide our customers with end-to-end service so that they can make the most of our solutions and stay protected against fraud.

We are committed to delivering the highest level of service and innovation to our customers, and we are confident that our integrated solution will help acquiring customers to minimize their risk and protect their digital transactions.



Navigating sophisticated transaction fraud trends in 2024

Kerry Thomas
Senior Vice President, Fraud & Decisioning
Products, Cyber and Intelligence Solutions (CAI)

In the ever-evolving landscape of transaction fraud trends, one thing remains constant — criminal activities are focused on manipulating consumer trends for maximum return. The trend of online shopping and bookings has seen a steady rise since 2021, creating a flourishing environment for fraudulent activity.

Let's explore six growing transaction fraud trends that will prepare you to safeguard your business and customers going forward.

A2A/P2P Fraud

The rise of account-to-account (A2A) and person-to-person (P2P) payment services has not gone unnoticed by fraudsters. These direct payment methods, fueled by the convenience they offer, are gaining their attention. Armed with stolen account and user information, fraudsters are devising strategies to exploit this burgeoning payments landscape.

Small online businesses and local market vendors frequently opt for A2A payments. However, this choice comes with an inherent risk. Fraudsters, adept at pilfering credentials, can use stolen information to acquire goods they later peddle on the black market.

> In an environment where trust is paramount, businesses must remain vigilant to protect both their reputations and their customers.

Online travel bookings

Spending on experiences rather than luxury goods is a trend we see carrying over into 2024. This presents an opening for opportunistic fraudsters: using counterfeit websites and deceptive social media advertisements to target thrifty travelers in search of attractive deals on flights and accommodations.

Statistics from the AARP indicate that 12% of respondents experienced a fraudulent travel booking if not made through reputable sources like airlines or established travel platforms.[30] A parallel risk extends to ticket resellers for major events. Fraudsters craft enticing websites offering heavily discounted flights, two-for-one deals and access to coveted events, such as Taylor Swift or Beyoncé concerts. These event tickets may be forgeries or legitimate ones acquired through stolen credit card details. When the fraud is inevitably uncovered, the purchased trip or event turns into a mere mirage.

Brushing scams

A familiar but resurging scheme in the world of transaction fraud is the "brushing scam." This term applies to the tales of unordered merchandise mysteriously appearing on people's doorsteps, containing mundane contents like potato peelers or tennis balls.

E-commerce's increasing popularity has breathed new life into brushing scams. Fraudsters establish websites to sell an assortment of products, shipping cheap, lightweight items to names and addresses gleaned from the internet. These items are often meticulously packaged using materials from established sellers, such as Amazon. On the fake vendor websites, these fraudulent transactions present as legitimate sales, garnering five-star reviews for the "received products."

Victims often find their names on review sites, despite never having initiated the purchases. Unsuspecting shoppers, lured by these positive reviews, subsequently place orders for more expensive items. By the time they realize they have been trapped by a scam, the fraudsters have already collected substantial sums and vanished into the digital ether.

Collusion for transaction fraud

The term "collusion" carries weight in the world of transaction fraud. This sophisticated form of fraud occurs when merchants form alliances with fraudsters, resulting in dire consequences for payment acquirers. Imagine a scenario where a struggling online toy store processes a staggering $1 million in sales during the holiday season. However, when products fail to arrive or are replaced with cheap alternatives, customers inevitably seek refunds. But by this time, the vendor has disappeared into the shadows, leaving angry customers in their wake.

Collusion occurs in various forms. It may involve two employees within a large corporation working in unison to divert a portion of sales revenue for personal gain, or it could be a criminal recruiting merchants into a web of deception, all in exchange for lucrative, tax-free sums. These covert collaborations often require time and advanced tools to be unearthed, making them a substantial threat.

Statistics from AARP indicate that **12%** of respondents experienced a fraudulent travel booking

Pig butchering

A particularly insidious form of transaction fraud that has gained traction is "pig butchering." This scam, a masterclass in social engineering, plays the long game, making it especially effective when individuals may be grappling with financial constraints and searching for quick solutions.

In a "pig butchering" scheme, fraudsters employ intricate tactics to dupe victims into investing substantial sums of money. Victims are promised a high return on a short-term investment, such as cryptocurrency or mortgage investments. Scammers generously dole out impressive interest payments, eliciting further investments from their targets. This process fattens up the unsuspecting investor, cultivating a sense of trust and fostering a history of legitimate returns. However, when the investor attempts to withdraw their funds, the fraudster disappears into the digital abyss, leaving the victim empty-handed and betrayed.

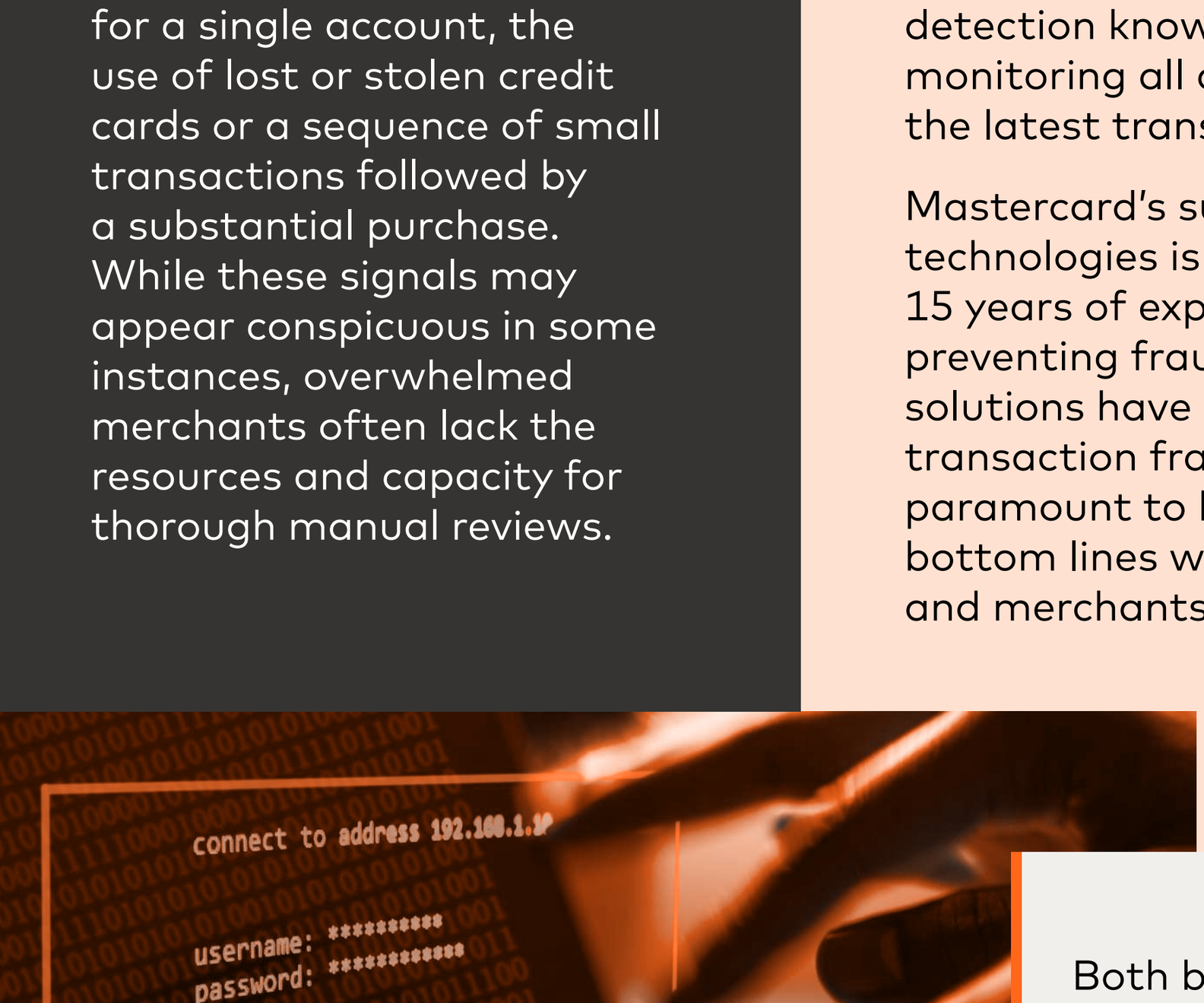
Fraud that happens in multiples

During busy seasons, merchants may inadvertently overlook the subtle indicators of fraudulent activities. These include an unusually high number of orders originating from the same IP address, multiple failed login attempts for a single account, the use of lost or stolen credit cards or a sequence of small transactions followed by a substantial purchase. While these signals may appear conspicuous in some instances, overwhelmed merchants often lack the resources and capacity for thorough manual reviews.

Vigilance and early detection are paramount for transaction fraud

In this ever-shifting landscape, vigilance and early detection are pivotal. The power of AI for fraud prevention has reached new heights. Industry leaders are training AI models using historical global intelligence, equipping them with the ability to predict and prevent fraud attempts earlier in the payment process. Organizations can significantly improve fraud detection knowing that their solution will be monitoring all anomalous behaviors, including the latest transaction fraud trends.

Mastercard's suite of AI fraud decisioning technologies is a prime example. With over 15 years of experience in identifying and preventing fraud in real time, Mastercard's AI solutions have become the gold standard in transaction fraud prevention. AI has become paramount to both issuers' and acquirers' bottom lines while also protecting consumers and merchants from nefarious actors.



Both businesses and consumers must remain mindful of the continuously evolving marketplace, a realm where even fraudsters adapt and thrive.

Sustainable cards for an environmentally conscious future

The adage “reduce, reuse, recycle” is more urgent now than ever. But around the world billions of plastic cards are produced each year, most of them from first-use plastics and not recycled materials.

Paul Trueman
Executive Vice President, Segment Intelligence and Engagement, Cyber and Intelligence Solutions (CAI)

Joe Pitcher
Vice President, Industry Standards, Cyber and Intelligence Solutions (CAI)

In line with our commitment to lead the industry in sustainability, Mastercard launched the Sustainable Card Program in 2018 as part of our Digital Security Lab’s Greener Payments Partnership. Designed to bring attention to plastic card waste and drive solutions at an industry level, the program has enrolled more than 490 issuers in 96 countries. Mastercard is working with major card manufacturers to transition all cards across its network to recycled and bio-based materials.

Now Mastercard has announced that beginning Jan. 1, 2028, all newly produced Mastercard plastic payment cards will be made from more sustainable materials — including recycled or bio-sourced plastics such as rPVC, rPET or PLA — and approved through a certification program, in a first move for a payment network.

Today, most payment cards are made from multiple sheets of polyvinyl chloride (PVC), which is difficult to recycle. Typically, a coiled wire antenna is sandwiched between these layers and an overlay is added to the back that contains a magnetic strip. In our sustainable cards, these layers are all made from recycled and bio-sourced materials. [See photo.] Our use of these materials, along with water or vegetable-based inks, will help cut pollution, reduce the space used in landfills and decrease demand for fossil fuels.

> **Progress is being made with millions of cards across the Mastercard network already consisting of sustainable materials.**

Why recycle?

- Reduces pollution across ecosystems
- Requires less energy and helps conserve natural resources
- Saves fast-depleting landfill space
- Eases demand on fossil fuel consumption
- Promotes a healthy and sustainable lifestyle

In another first, beginning in 2028, all new cards on our network will be required to pass certification at our state-of-the-art Digital Security Lab in the United Kingdom. The rigorous evaluation will ensure that they are made from sustainable materials, secure and strong enough to withstand the rigors of thousands of taps and swipes. And progress is being made with millions of cards across the Mastercard network already consisting of sustainable materials.

Social responsibility has become a staple in many industries and businesses, as companies introduce Environmental, Social and Governance (ESG) goals and hold themselves accountable. Our sustainable cards will help issuers achieve their ESG goals, allowing us to continue building on our established partnerships and create new ones. Mastercard has also formed partnerships to help our customers collect and recycle their cards. In addition to enabling a circular economy, this will encourage issuers to align their own ESG initiatives with local or market partners.

We are setting a new industry standard by helping Mastercard issuers reduce their carbon footprint.

Everyone has a vested interest in the health of our environment. Our actions today will determine what happens decades from now. Mastercard is leading by example to ensure that our planet has a cleaner future.

Mastercard's RiskX: Navigating the future of cybersecurity and trust

Robyn Tompkins
Vice President, Product Management,
Cyber and Intelligence Solutions (CAI)

Mastercard's RiskX conference — our key customer and partner event — was held in the vibrant and historic city of Barcelona, Spain, in October 2023. We brought together industry experts, thought leaders in tech and cybersecurity enthusiasts to discuss the latest developments in the world of digital security.

The event focused on what our world is buzzing about today: artificial intelligence, identity verification and the ongoing battle against cyberthreats. The lineup of speakers, who ranged from entrepreneurs to industry leaders with deep expertise in AI, sparked engaging discussions that explored the fascinating and complex world of cybersecurity and risk management.

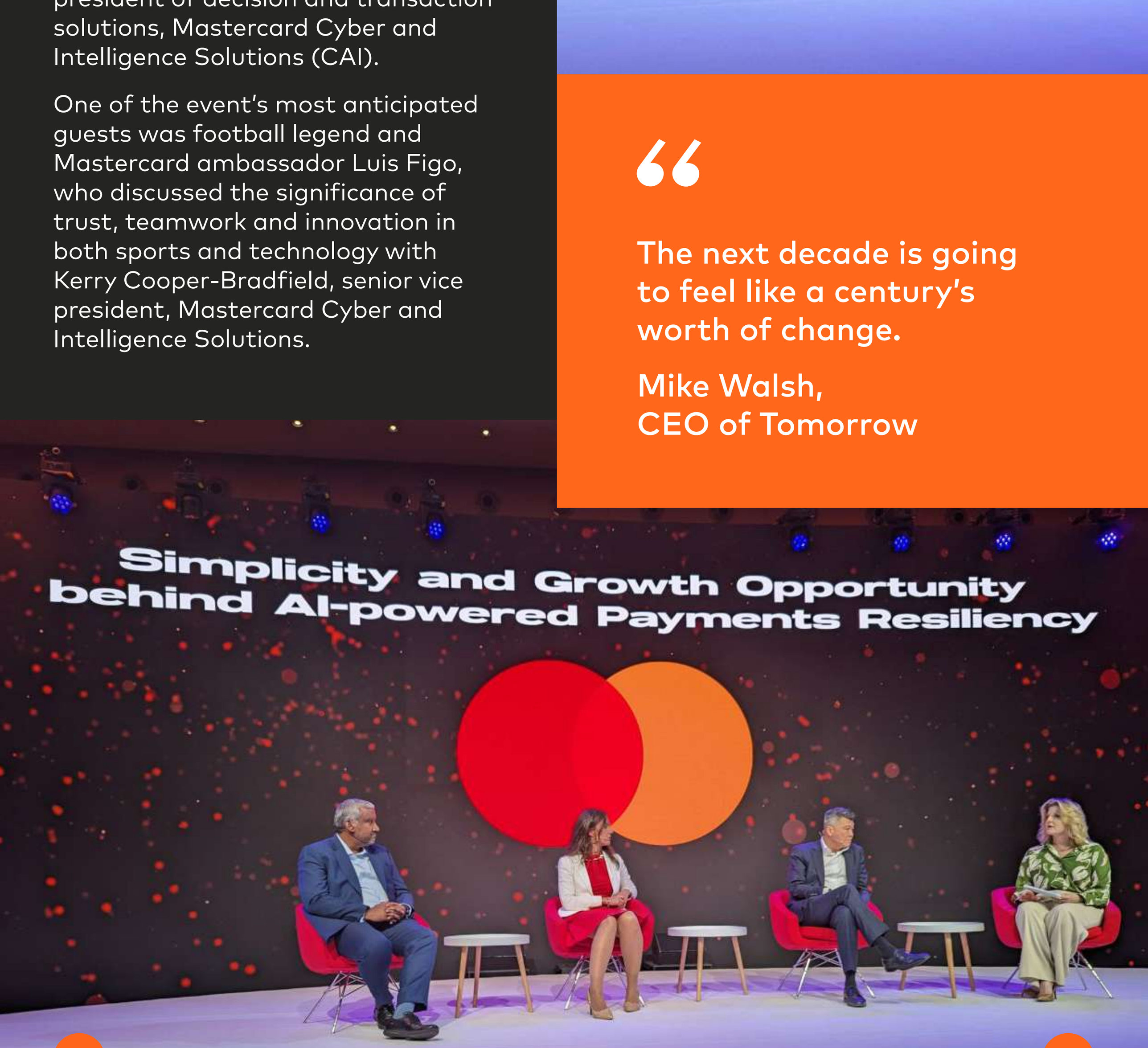
Day one kicked off with a captivating presentation by futurist Mike Walsh, CEO of Tomorrow, who highlighted the pivotal role of AI in shaping our future. He emphasized that the next decade will bring a century's worth of change, underscoring the urgency of staying current — and not complacent — with today's fast-changing shifts in technology.

Next, Ajay Bhalla, president, Mastercard Cyber & Intelligence, engaged in a thoughtful conversation with Bhaskar Chakravorti, dean of global business at The Fletcher School, Tufts University, shedding light on the transformative power of AI in the payments industry. Johan Gerber, executive vice president, Mastercard Cyber and Security Products, and retired U.S. Army Gen. Keith Alexander then took to the stage to explore the importance of data security and AI in safeguarding the digital ecosystem, emphasizing the necessity of collaboration across industries and borders to counter cyberthreats.

Attendees also learned about innovation during uncertain times from futurist and innovation expert Angela Oguntala and discovered new insights about AI-powered payment resiliency with Laura Quevedo, executive vice president of decision and transaction solutions, Mastercard Cyber and Intelligence Solutions (CAI).

One of the event's most anticipated guests was football legend and Mastercard ambassador Luis Figo, who discussed the significance of trust, teamwork and innovation in both sports and technology with Kerry Cooper-Bradfield, senior vice president, Mastercard Cyber and Intelligence Solutions.

> The next decade is going to feel like a century's worth of change.
>
> Mike Walsh,
> CEO of Tomorrow



Day two commenced with a thought-provoking presentation by mathematician Hannah Fry, who urged participants to critically examine the intersection of humanity and technology for a brighter future. Chris Reid, executive vice president, Mastercard Identity Solutions, then delved into creating a trusted and frictionless customer experience while maintaining rigorous security standards.

After that, Gerber joined rugby legend Bryan Habana in a fireside chat where Habana offered intriguing insights into leadership, transferrable skills and the importance of rugby as a unifying force in his home country of South Africa.

The keynote presentations concluded with a powerful fireside chat with bestselling author and entrepreneur Steven Bartlett, who emphasized the significance of challenging the status quo and continually seeking ways to outperform the competition.

Bhalla best captured the spirit of the event with these words: "Whether on the football pitch or in the workplace, being teammates or colleagues with people who speak different languages and come from diverse backgrounds creates opportunities and the need for trust. It's only with trust that you can create the environment for growth, peak performance and, most importantly, achieving your goals."

RiskX 2023 was an unforgettable meeting of the minds. It also offered an essential forum for networking and knowledge-sharing in our collective and ongoing quest to secure trust in the digital economy.

Be sure to stay tuned for updates on RiskX 2024 in the coming weeks!

RiskX 2023 was an unforgettable meeting of the minds, offering an essential forum for networking and knowledge-sharing.

Notes

ACCESS

1 Deloitte, Global Cost Report 2019-2020, "Save-to-transform as a catalyst for embracing digital disruption Deloitte's second biennial global cost survey," April 2019

2 SecurityInfo, A Brief History of Machine Learning in Cybersecurity, November 2019

3 Javelin Research, 2022 Identity Fraud Study, "The Virtual Battleground," March 2022

4 Javelin Research, 2023 Identity Fraud Study, "The Butterfly Effect," March 2023

5 FIS, "Global Payments Report 2023," May 2023

6 The Global Anti-Scam Alliance, "Global State of Scams 2023 Report," March 2023

7 Mastercard, "A2A payments trends, risks and fraud solutions," May 2023

8 The Federal Trade Commission, "Social media: a golden goose for scammers," October 2023

CYBER

9 https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud →

10 https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf →

11 Europol (2021), Cryptocurrencies - Tracing the evolution of criminal finances, Europol Spotlight Report series, Publications Office of the European Union, Luxembourg →

12 The FTC's mission is to protect consumers and competition by preventing anticompetitive, deceptive, and unfair business practices through law enforcement, advocacy, and education without unduly burdening legitimate business activity →

13 https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze →

14 The FBI issued a warning to investors and financial institutions about cyber criminals creating fraudulent cryptocurrency investment applications (apps) to defraud cryptocurrency investors. 244 victims have been scammed who have lost about $42.7 million →

15 https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze →

16 https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/romance-scams →

17 https://www.ic3.gov/Media/Y2021/PSA210916 →

18 https://brighterion.com/merchant-fraud-predictions-for-2022-a-pandemic-driven-increase/ →

19 https://www.synovus.com/personal/resource-center/financial-safety-and-security/types-of-credit-card-fraud/ →

20 CipherTrace Cryptocurrency Crime and Anti-Money Laundering Report June 2022

21 https://www.ic3.gov/Media/News/2022/220718.pdf →

22 https://www.techtarget.com/whatis/feature/Common-cryptocurrency-scams →

IDENTITY

23 Mastercard Spending Pulse, September 19, 2023 →

24 Salesforce 2023 Holiday Forecast, August 23, 2023 →

25 Digital Holiday Fraud in 2022, TransUnion, December 2022 →

26 Online Payment Fraud Market Report 2023-2028, Juniper Research →

27 An (Un)necessary Tradeoff: Fraud Prevention Strategies Should Enhance, Not Compromise, Customer Experience, Frost & Sullivan in partnership with Ekata, 2021 →

28 Online Marketplace Fraud Trends 2021, Ravelin →

29 Navigating new chargeback complexities in eCommerce, Merchant Risk Council, March 22, 2023 →

RISK & RESILIENCY

30 https://www.aarp.org/money/scams-fraud/info-2023/holiday-consumer-survey.html →

For more information visit:

b2b.mastercard.com

Or contact your Mastercard representative.

LinkedIn