WHITE PAPER
NOVEMBER 2024

Securing the digital ecosystem with AI

AI's impact on payments and beyond

Contents

Executive summary

Rohit Chauhan
Executive Vice President, AI-Fraud Solutions
Mastercard

"In an era where our digital ecosystem continues to expand at an unprecedented rate, understanding and mitigating the associated risks has never been greater.

Securing the digital ecosystem with AI delves into the profound impact of artificial intelligence (AI) on the financial landscape, particularly focusing on its ethical use and governance. As we leverage AI to streamline operations and enhance our products, it is imperative that we also address ethical considerations and establish robust governance frameworks. This dual approach not only secures the future of AI but also fortifies the trust our customers place in us.

The benefits of AI are enterprise-wide, spanning from predictive analytics to anomaly detection. However, with these advancements come new challenges. The digital ecosystem presents fertile ground for criminal activities, with interconnected payment systems and vast online data repositories. Alarmingly, global fraud losses surpassed $485 billion in 2023[1], a figure projected to escalate as fraudsters exploit generative AI to launch more sophisticated attacks.

In response, a significant majority of financial institutions are ramping up their technology investments, prioritizing fraud detection and data-sharing initiatives. This proactive stance is crucial in building a resilient payments ecosystem capable of withstanding the evolving threats.

It is equally important to be educated on the different types of fraud to recognize suspicious activity — from phishing and identity theft to more sophisticated AI-driven schemes. By being informed, we can appreciate the critical role AI plays in combating fraud and how its implementation helps safeguard transactions and personal information.

As you review the insights presented in *Securing the digital ecosystem with AI*, I encourage you to consider the broader implications of AI within your organizations. Embrace the transformative potential of AI but do so with a commitment to ethical practices and rigorous governance.

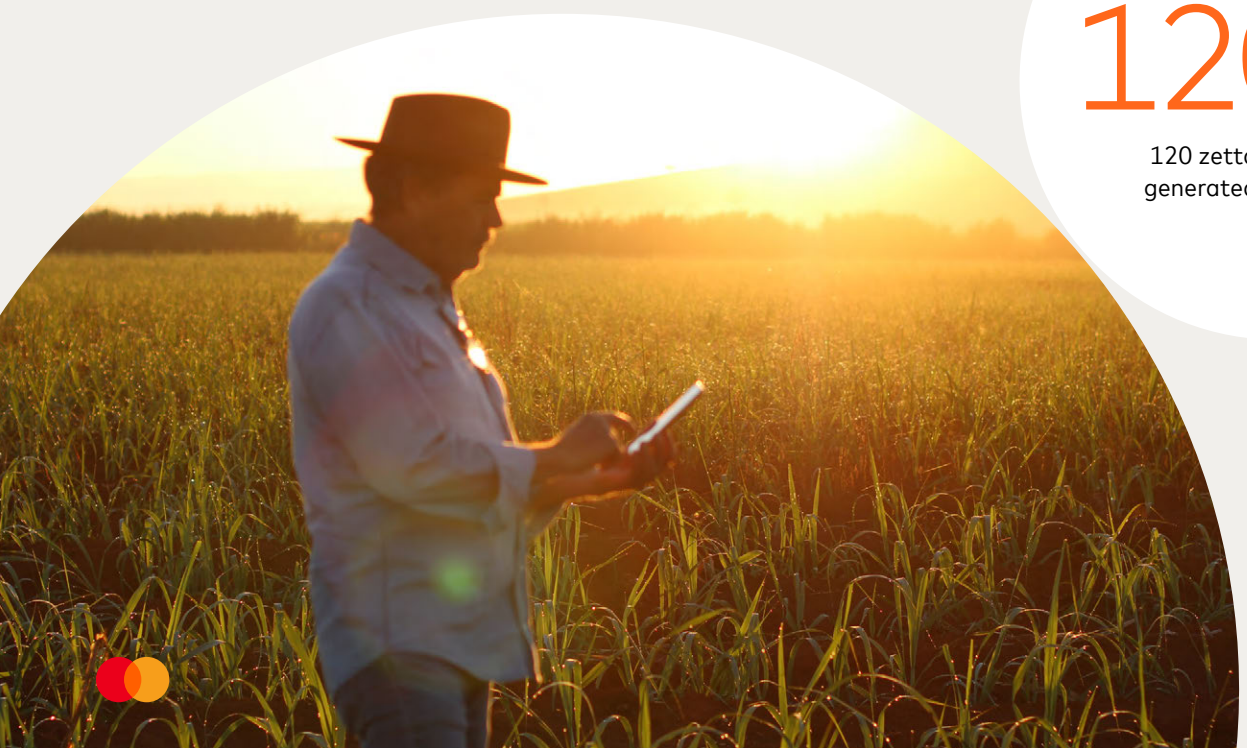
Our collective actions today will pave the way for a secure and innovative future, one where trust remains the cornerstone of our industry.

AI and the digital ecosystem: Understanding new dynamics

As the defining technology of our time, AI offers powerful solutions to some of the world's most complex challenges while augmenting human capabilities. By expertly processing vast amounts of data with speed and precision, AI enables breakthroughs that were once unimaginable and makes predictions that drive innovation and positive change. As the world becomes increasingly connected online, this technology is critical in enhancing human decision-making and helping businesses navigate the complexities of modern commerce and finance. At the same time, it unlocks opportunities for meaningful social impact.

Digital commerce is projected to reach $20 trillion in transactions by 2027[2] and is essential to the global economy. As internet users surge,[3] more people globally are opening bank accounts, embracing e-commerce and adopting seamless payment methods for everyday transactions, which in turn expands the digital ecosystem. Financial institutions operate at the core of this new ecosystem, facilitating secure commerce across manufacturing, agriculture, retail, healthcare and government sectors.

In growing markets, such as India, governments play a key role in financial inclusion and fostering competition.[4] In Latin America, digital payments are gaining popularity, fueled by consumer demand and e-commerce growth.[5] Globally, the adoption of digital banking continues to rise, driven by the increase of digital-only banks and ongoing transformations within established institutions.[6] This rapid shift has contributed to massive data growth, with an estimated 120 zettabytes generated in 2023 alone.[7] Every click and transaction feeds this expanding ecosystem, presenting organizations with opportunities and risks.



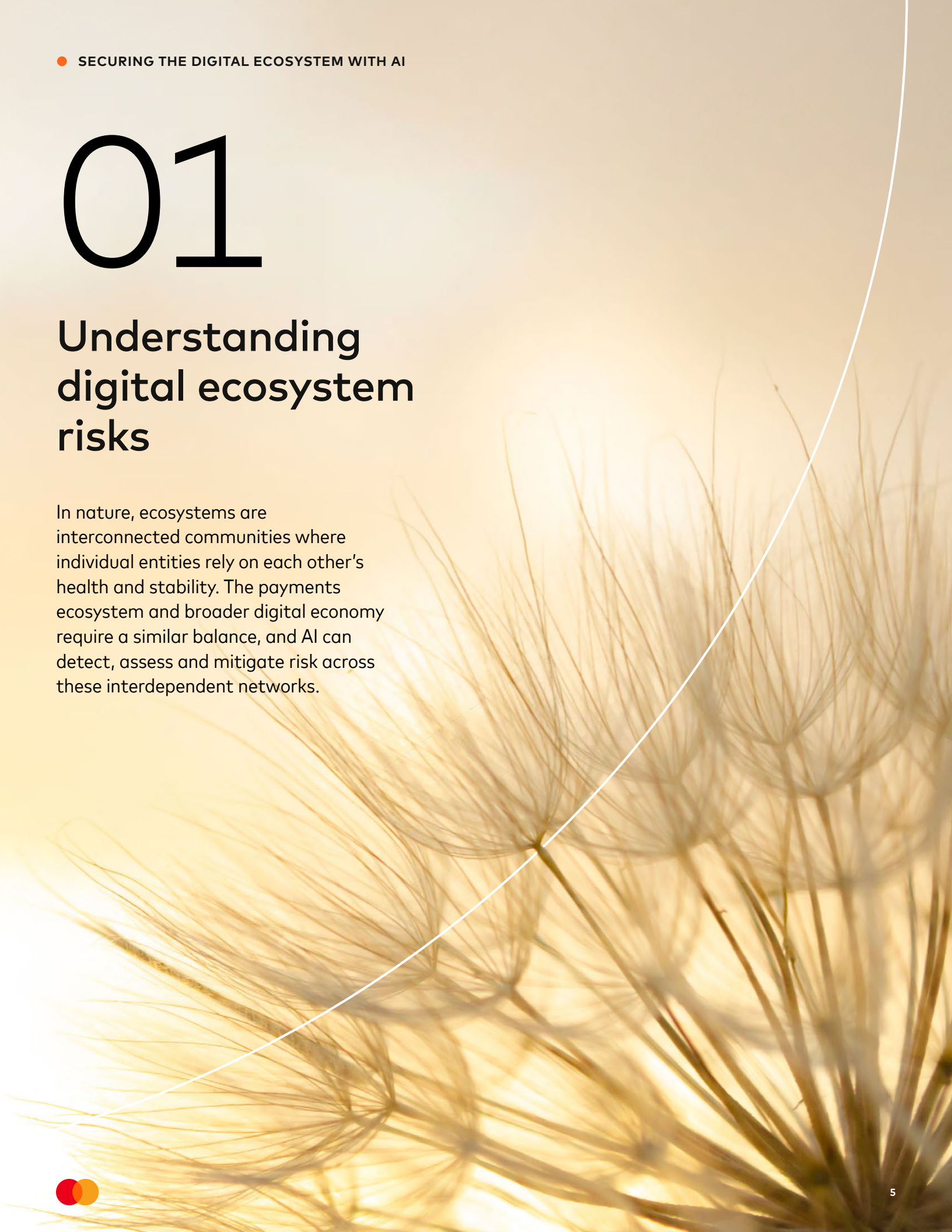
120zb

120 zettabytes of data generated in 2023 alone

01

Understanding digital ecosystem risks

In nature, ecosystems are interconnected communities where individual entities rely on each other's health and stability. The payments ecosystem and broader digital economy require a similar balance, and AI can detect, assess and mitigate risk across these interdependent networks.



The cycle of fraud

Cyber attacks against critical, high profile industries

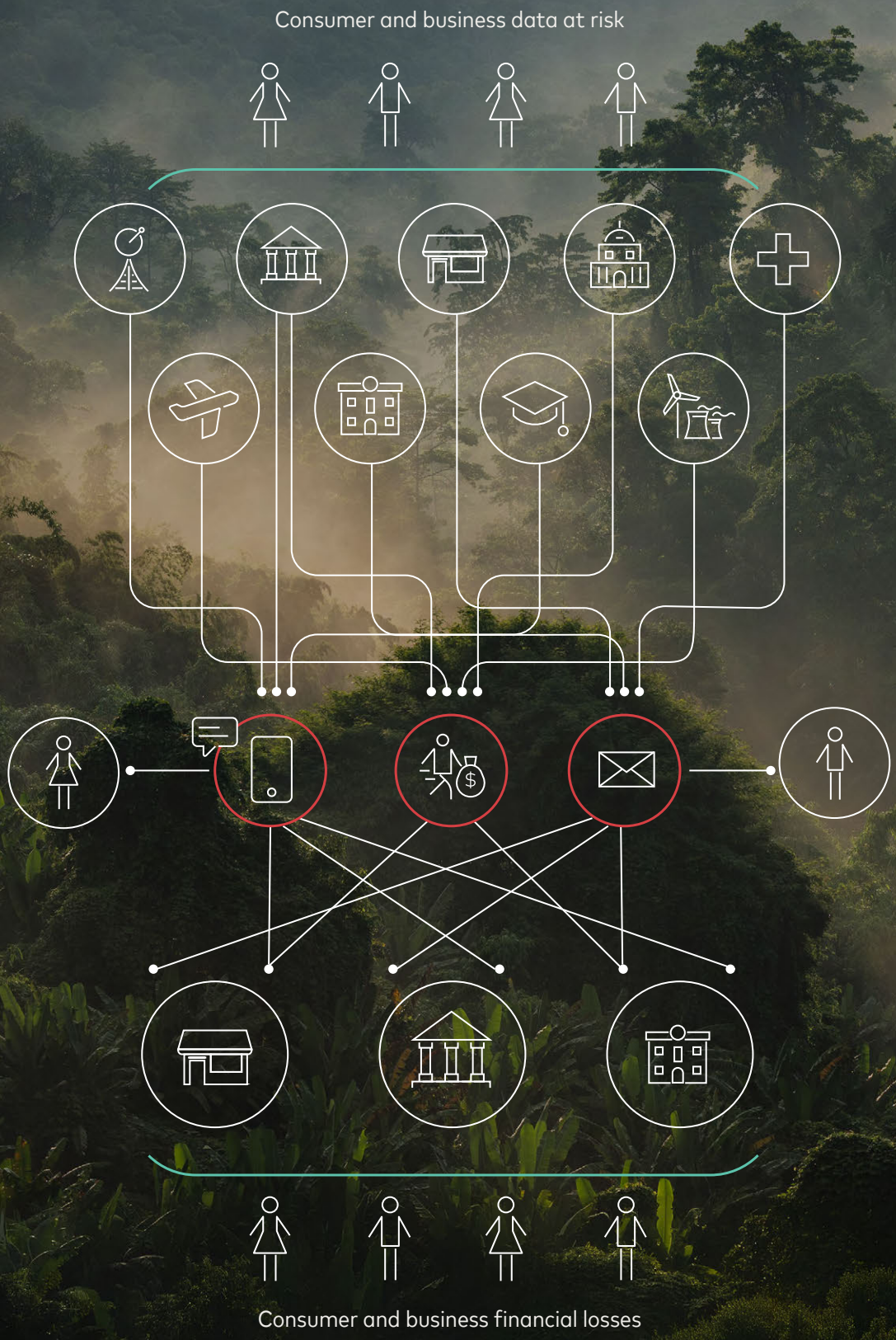
- Telecommunications
- Financial institutions
- Merchants
- Governments
- Healthcare
- Travel
- Education
- Energy

Direct attacks on consumers

- Social engineering
- Phishing
- Text scams

Fraud attacks on the payments ecosystem

- Data from breaches fuel consumer attacks, resulting in large-scale fraud using advanced technologies.



Must-know trends

$485b
Global fraud losses in 2023

$40b
Fraud losses in the U.S. by 2027

80%
of financial institutions plan to increase their technology spending

As the digital ecosystem grows, criminals find more opportunities to exploit vulnerabilities. Interconnected payment systems and ever-expanding online data have broadened the attack surface, increasing the risk and complexity of fraud.

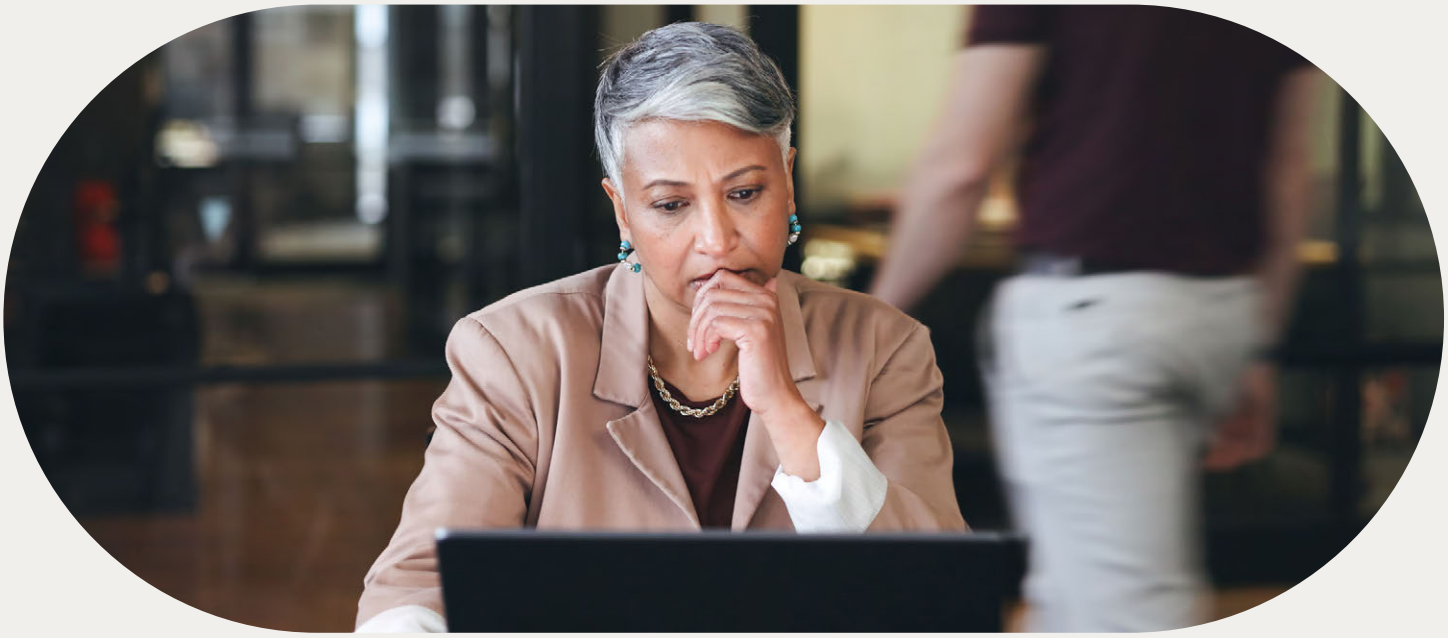
The cost of fraud

The global impact of fraud is staggering, with losses exceeding $485 billion in 2023.[8] Fraud-as-a-service models have lowered the barriers to entry, allowing even those with minimal technical expertise to launch attacks. This threat is accelerating with Generative AI (GenAI). In the United States (U.S.), fraud losses could rise to $40 billion by 2027, up from $12.3 billion in 2023,[9] as GenAI makes attacks more convincing, widespread and difficult to detect.

Investing in the future

According to a recent study, 80% of financial institutions plan to increase their technology spending significantly in the next two years, with fraud detection as a top priority.[10] Additionally, the need for better information and data-sharing is becoming more recognized.

These trends highlight a growing awareness of fraud risks and an emphasis on proactive, collaborative efforts to protect the payments ecosystem.

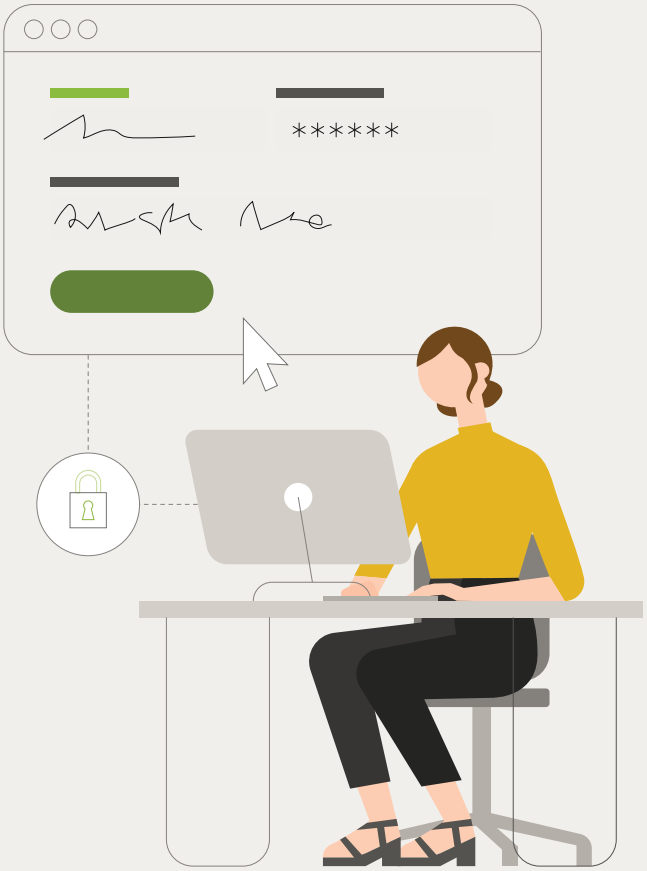


Cybersecurity challenges

Cyber attacks

Fraud often begins with cyber attacks targeting diverse industries across the digital landscape. Organizations with a rich pool of personal data combined with weak cybersecurity make them an easy target for cyber attacks.

Breaches are on the rise, with stolen credentials quickly becoming the most common gateway into victims' systems, surging 71% year-over-year.[11] Non-financial breaches can expose sensitive data, such as social security numbers, addresses, and birthdates, which criminals later exploit for financial fraud. This trend makes it easier for criminals to exploit valid accounts, increasing the vulnerability of the financial ecosystem.



Key cybersecurity risks include:

Malware
A type of harmful software designed to infiltrate or damage digital systems, often installed unknowingly onto a computer, server or mobile device. Malware includes viruses, ransomware, spyware and Trojans. Malware enables criminals to steal personal information that is later used in attacks.

Ransomware attacks, which demand payment for decrypting systems, are rising. These attacks disproportionately target the healthcare industry,[12] with ransomware-as-a-service models enabling more sophisticated, scalable attacks.

Third-party risks
Vulnerabilities in third-party vendors or suppliers can compromise entire supply chains, multiplying risk as more interconnected services are affected.

Social engineering
Techniques such as impersonation or Business Email Compromise (BEC) trick individuals into divulging sensitive information. Even seemingly harmless details shared on social media can help attackers craft highly convincing, targeted schemes that help bypass technical defenses.

Phishing
A common precursor to ransomware and other attacks, these mass-targeted scams deceive users into sharing personal information, granting criminals access.

Fraud risks

Payment fraud

Today, the payments ecosystem faces diverse fraud tactics, further exacerbated by emerging payment types such as cryptocurrency and real-time payments. These newer vulnerabilities add complexity due to their anonymity and the irreversibility of transactions.

Payment fraud is a significant threat, as fraudsters continuously adapt their methods across multiple channels. The rise of omnichannel banking — including online banking, mobile apps, and call centers — has expanded the attack surface, making it difficult for organizations to secure each entry point. Here are some of the most pressing risks:

Account Takeover (ATO)
Criminals traditionally use techniques such as password sniffing, credential stuffing, or phishing to gain access to an account. Once inside, they quickly make unauthorized transactions or drain funds before the victim is even aware. The availability of GenAI, and malicious tools such as WormGPT and FraudGPT, allows criminals to easily scale phishing and malware attacks.

More recently, fraudsters are stealing facial recognition data to bypass security checks and access bank accounts, as seen in recent campaigns by hackers in Southeast Asia.[13]

In addition to direct attacks, third-party ATO attacks are increasing, with data showing an 18% year-over-year increase in attacks in 2023, following a 52% year-over-year increase in 2022.[14]

Transaction fraud
There are many shades of transaction fraud. One major concern is fraudsters' use of advanced methods to exploit stolen credit card data. These details, often acquired from breaches or fake merchant websites that harvest card credentials, result in costly chargebacks.[15] Fraud often goes undetected until post-authorization, leading merchants to ship goods that are later disputed, causing financial losses and unfilled orders.

Bank Identification Number (BIN) attacks
A particularly concerning type of transaction fraud is BIN attacks — where fraudsters use automated software to systematically test card numbers within a BIN to identify valid combinations. These attacks have surged by 80% globally since 2020.[16]

Account onboarding and identity fraud
Fraudsters continue to exploit onboarding processes using stolen or fabricated identities to open bank accounts or pose as legitimate merchants. Synthetic identity fraud, which combines real and falsified information to create new identities, is particularly challenging to detect[17] and is the fastest-growing financial crime in the U.S.[18]

GenAI and deep fakes exacerbate this threat by producing synthetic imagery and making fake identification documents difficult for fraud teams to detect during account onboarding and Know Your Customer checks. In some cases, fraudsters even spoof biometric data.[19]

To avoid detection, fraudsters often keep synthetic identity accounts dormant for months or years, securing good credit lines before committing bust-out fraud, where they max out credit and disappear without repayment.[20]

$1.14b

reportedly lost to romance scams in the U.S.

Merchant fraud

Fraud by merchants is increasingly prevalent in the payments ecosystem as opening merchant accounts has become easier. Payment facilitators create thousands of new accounts daily, giving organized criminals opportunities to exploit the system and illegally open accounts for fraudulent activities.[21] Fake merchant accounts can process purchases from stolen credit card information, defrauding issuers and leading to chargebacks.

In some cases, individuals listed on anti-money laundering (AML) or anti-terrorist financing watchlists, or those originating from countries with economic sanctions, create merchant accounts using stolen or synthetic identities. Regulators expect acquirers to perform due diligence to prevent these activities, or face fines and reputational damage.[22]

AML and regulatory compliance

Criminals exploit financial systems to launder money from illegal activities through placement, layering, and structuring. While financial institutions and other regulated businesses have systems to detect and prevent money laundering, traditional rules-based approaches often fail to keep up with increasingly sophisticated schemes – leading to high false-positive rates and overlooked threats. These static methods overwhelm compliance teams, diverting their focus from genuinely suspicious activities.

Businesses need advanced systems to detect and prevent money laundering by analyzing transaction patterns and network connections. For example, tactics such as money muling obscure the origin of illicit funds by layering transactions under the guise of legitimate activities. Modern AI-based tools can analyze real-time data and networks, spotting anomalies or hidden patterns that traditional systems miss.

While AML regulations become more stringent worldwide, the payments ecosystem needs adaptable, effective systems to meet compliance — or risk fines and exposure to escalating threats.

Account-to-Account (A2A) scams

A2A scams, which involve payments that move directly from one account to another without using payment cards, have grown in popularity since 2020.[23] They can stem from unauthorized account access, as seen in ATO fraud or manipulation techniques that prey on human vulnerabilities.

These scams include peer-to-peer, consumer-to-business and business-to-business payment services.

Following rapid growth, A2A scams are difficult to prevent. Common risk factors include:

- **Social engineering:** Fraudsters trick customers into transferring funds or forfeiting sensitive information through emotional tactics, such as romance scams, investment or boiler room schemes, sextortion or impersonation scams. In the U.S., reported losses to romance scams totaled $1.14 billion in 2023.[24]
- **Authorized push payment (APP) fraud:** Fraudsters deceive victims into authorizing payments under pretenses, often posing as a bank or government authority. Once the transfer is complete, victims may struggle to recover their money since they willingly authorized the transaction. Sometimes, deep fake technology mimics a loved one's voice, making the scam even more convincing. Payment and financial service providers are increasingly feeling pressure to refund victims, with proposed legislation in the U.S.[25] and regulations already in place in the United Kingdom.[26]
- **Me-to-Me fraud:** The scheme involves a scammer manipulating a victim into moving funds between their accounts, often across different institutions, into a single compromised account. Once the funds are consolidated into an account the fraudster controls, they steal the money.

Operational challenges and opportunities

Data fragmentation

Data fragmentation within the payments ecosystem makes fraud prevention and detection more difficult, increasing financial losses. Many financial institutions have data silos, which present an incomplete picture for detecting patterns and gaining a full understanding of fraud risk.

Typically, financial institutions rely on up to 20 different technology solutions across various departments, with multiple parties involved in a single transaction.[27] For example, a typical credit card transaction usually involves the issuer, merchant, acquirer, payment service provider, and card network. Because these parties are distinct, they only have partial visibility into the customer, limiting the ability for a comprehensive risk assessment.

A unified approach

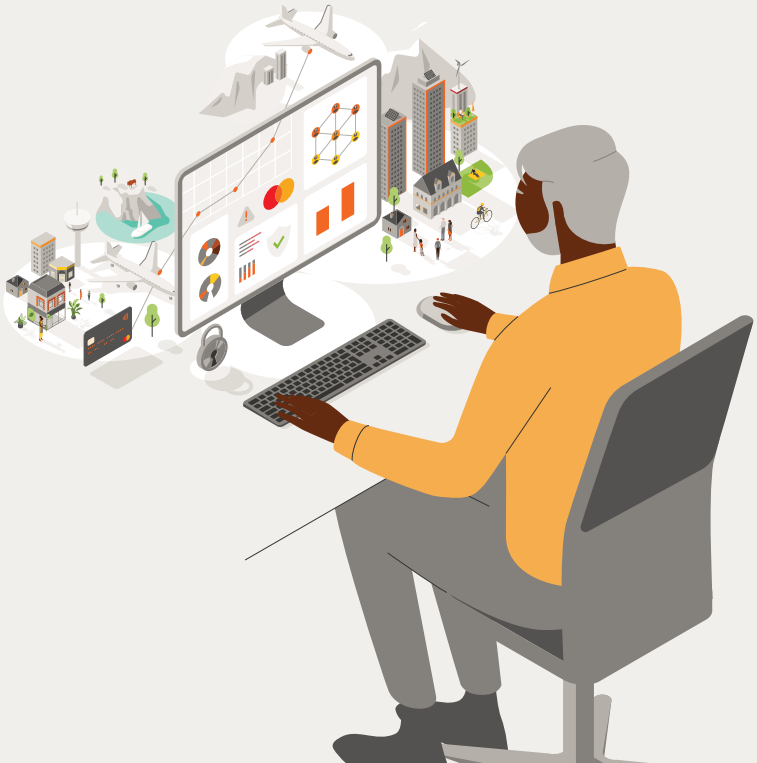
To address data fragmentation, better information sharing across departments and organizations is critical. Unifying data and insights from disparate systems offers a clearer picture of customer behavior and transaction patterns. In turn, this holistic view fosters more proactive and real-time fraud detection. Using technology to consolidate data strengthens defenses and supports an effective, actionable fraud risk management strategy.

Beyond payments

Beyond payments, collaboration among governments, businesses and technology leaders is essential to coordinate effective efforts against cybercrime and fraud. Reducing cyber risk and safeguarding consumer data across the digital ecosystem strengthens collective defenses. While skilled workforces continue to advance AI and technology, the power of these innovations lies in the intelligence driving them.

At Mastercard, global businesses and consumers trust us with their data and intelligence spanning 210 countries and territories. In 2023 alone, we processed 143.2 billion secure transactions, working with over 3,900 businesses worldwide across diverse sectors. This breadth expands our view and impact far beyond payments. With this intelligence, our advanced AI solutions recognize global patterns and behaviors, giving us a truly unique perspective.

If more players in the ecosystem shared insights and intelligence with trusted solution providers, we could make greater strides in the fight against fraud.



02

How AI is used to reduce digital ecosystem risks

Today, AI is a transformative force, redefining what's possible at the intersection of speed and scale. Success in this space requires bold leadership and seamless coordination, with every move synchronized to harness the power of data and innovation.

Cyber attacks

AI and advanced technologies have become crucial tools to combat increasingly sophisticated criminal schemes. Just as criminals use AI to deploy attacks, businesses in the payments ecosystem must use the same technology to stay ahead.

Reinforcing cyber defense

As part of the cycle of fraud, fortifying cyber defenses across the digital landscape is vital to protect the payments ecosystem. The growing threat of data breaches and ransomware, especially its impact on supply chains, makes third-party risk management (TPRM) crucial for businesses.

AI tools aid cybersecurity measures through advanced anomaly detection and behavioral analysis techniques to reinforce measures such as endpoint protection, intrusion detection and prevention, data loss prevention, and firewall systems.[28] These AI systems can proactively identify and alert organizations to vulnerabilities, helping prevent attacks.

As cyber threats grow in complexity, AI's data-driven insights create more targeted defenses. These tools help businesses pinpoint and address vulnerabilities before criminals exploit them.

GEN AI IN ACTION

GenAI can predict card fraud from data breaches

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

Fraud

AI has critical capabilities that make it exceptional at combating fraud:

Pattern recognition: AI scans large data sets, pinpointing outliers, patterns and connections humans might miss. For example, it can spot money mule activity within vast datasets, often consisting of small, equal-amount transfers that are otherwise difficult to identify.

Predictive analysis: Using a company's historical data, strengthened by global datasets, AI can predict the likelihood of potential fraud or other behaviors, helping businesses instill proactive measures. This includes methods like time-series forecasting, where AI looks at transaction patterns over time to spot irregularities before they escalate into fraud.

Continuous learning: Machine learning, a subset of AI that relies on input and patterns from past data, allows AI systems to adapt and improve over time, becoming more accurate with every piece of new information. This continuous adaptation ensures that the system can respond to emerging fraud tactics and schemes — critical in the fast-paced world of fraud.

Graph neural networks/GenAI: Alongside traditional AI models, GenAI can produce rule recommendations for risk-scoring models using inputs like past transactions, decisions made by investigators, and consortium data. Additionally, data scientists can generate synthetic fraudulent activities to enhance the defensive capabilities of risk-score models.[30]

GEN AI IN ACTION

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

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

Training AI for optimal performance

AI efficiently addresses and anticipates potential threats, bolstering fraud defenses as part of a proactive approach. Central to this approach is the ability to analyze immense volumes of data to detect even subtle fraud patterns.

Because of these advanced capabilities, financial institutions today acknowledge that adopting AI, including GenAI, can improve the effectiveness and cost efficiency of their cybersecurity and anti-fraud efforts.[31]

Training models with sufficient, high-quality data are crucial to AI's effectiveness. It requires insights from extensive, diverse sources, building a form of global intelligence that supports accuracy. Mastercard's AI models are built on unique insights, resulting in a robust foundation for fraud detection.

In the case of transaction fraud detection, specifically, Mastercard's AI models are pre-trained offline, with regular updates, keeping them effective in real-time environments despite large data volumes. This approach allows organizations to make instant, data-driven decisions, maintaining the speed and accuracy of effective fraud prevention.

Layering AI solutions

Issuers, fintechs, acquirers, payment service providers, payment facilitators and merchants face similar risks at different stages of the digital experience, though each has unique criteria and requirements. Additionally, laws and compliance regulations vary across regions and territories, adding layers of complexity to data use and technology deployment.

Part One outlined that payment fraud takes many forms. Organizations need to deploy AI solutions to address these risks comprehensively — from account opening and credit assessments to consumer identity verification, merchant ID checks, transaction monitoring and chargeback mitigation.

AI IN ACTION

Mastercard's powerful platform: Brighterion AI

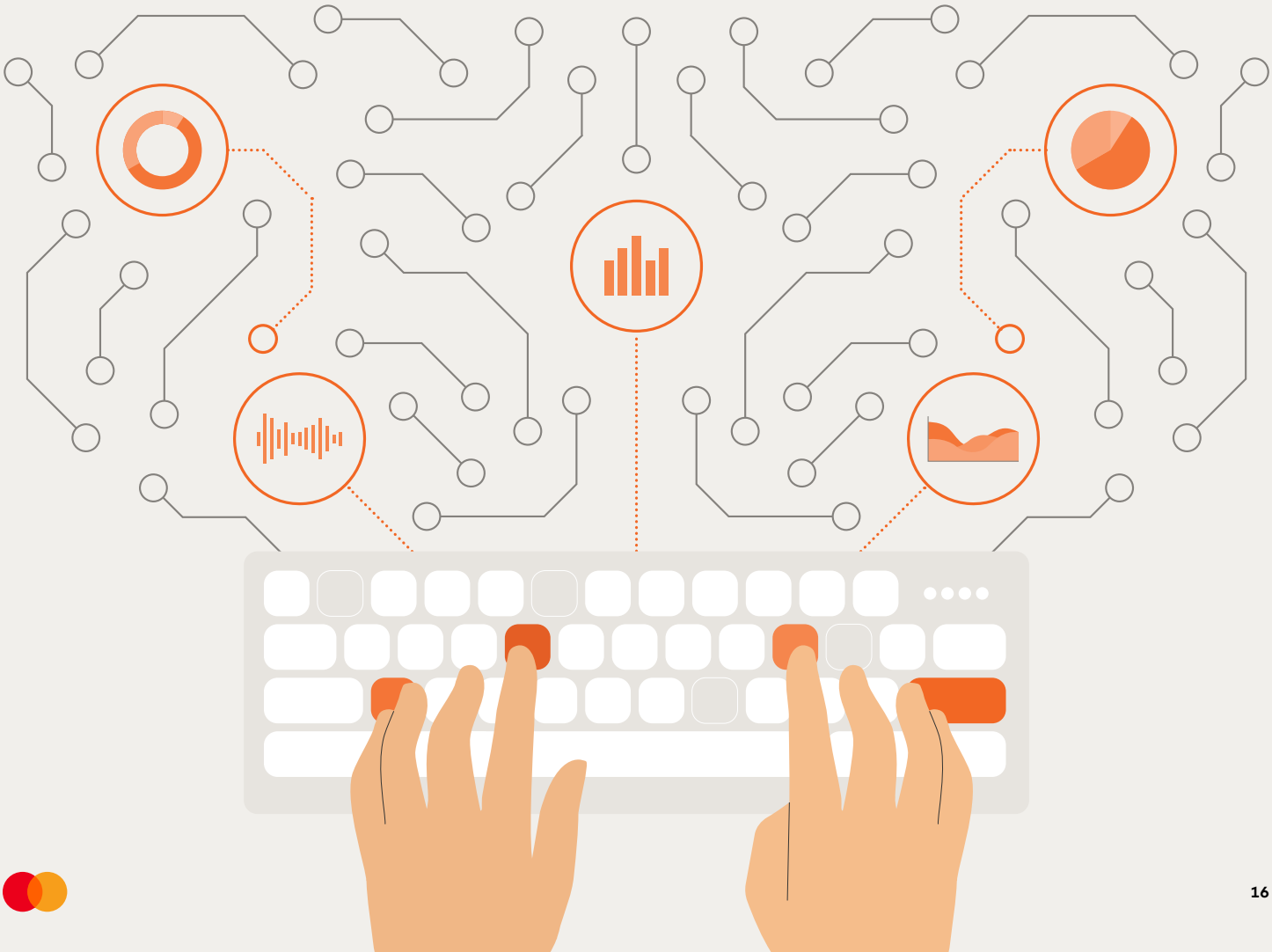
The Brighterion AI platform helps secure the payments ecosystem with advanced solutions for onboarding, merchant monitoring, and transaction monitoring across pre-authorization and post-authorization stages. Powered by global transaction intelligence, Brighterion AI solutions deliver reliable decisions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

Scams

Scams

AI-powered decision-making helps financial institutions detect scams, especially in A2A real-time transactions. Using models built on an institution's historical data — and supported by comprehensive data intelligence from across the digital ecosystem — AI can accurately score transactions based on their likelihood of being a scam. Through behavioral analysis of both senders and receivers, AI analyzes typical transaction patterns associated with each account. This allows the system to identify out-of-pattern transactions, giving financial institutions insights into potential scams or fraudulent activities.

By synthesizing diverse inputs — such as transaction history, behavioral and biometric patterns, identity data and device identification — AI functions as an orchestration engine, assessing risks through a multi-layered approach. The real-time nature of this process is important for timely detection and interference of suspicious activity.



Enterprise-wide benefits

Efficiency gains

More precise fraud detection translates to greater operational efficiencies, reducing the likelihood of false positives and unnecessary manual reviews or processes. This, in turn, drives overall productivity across the organization.

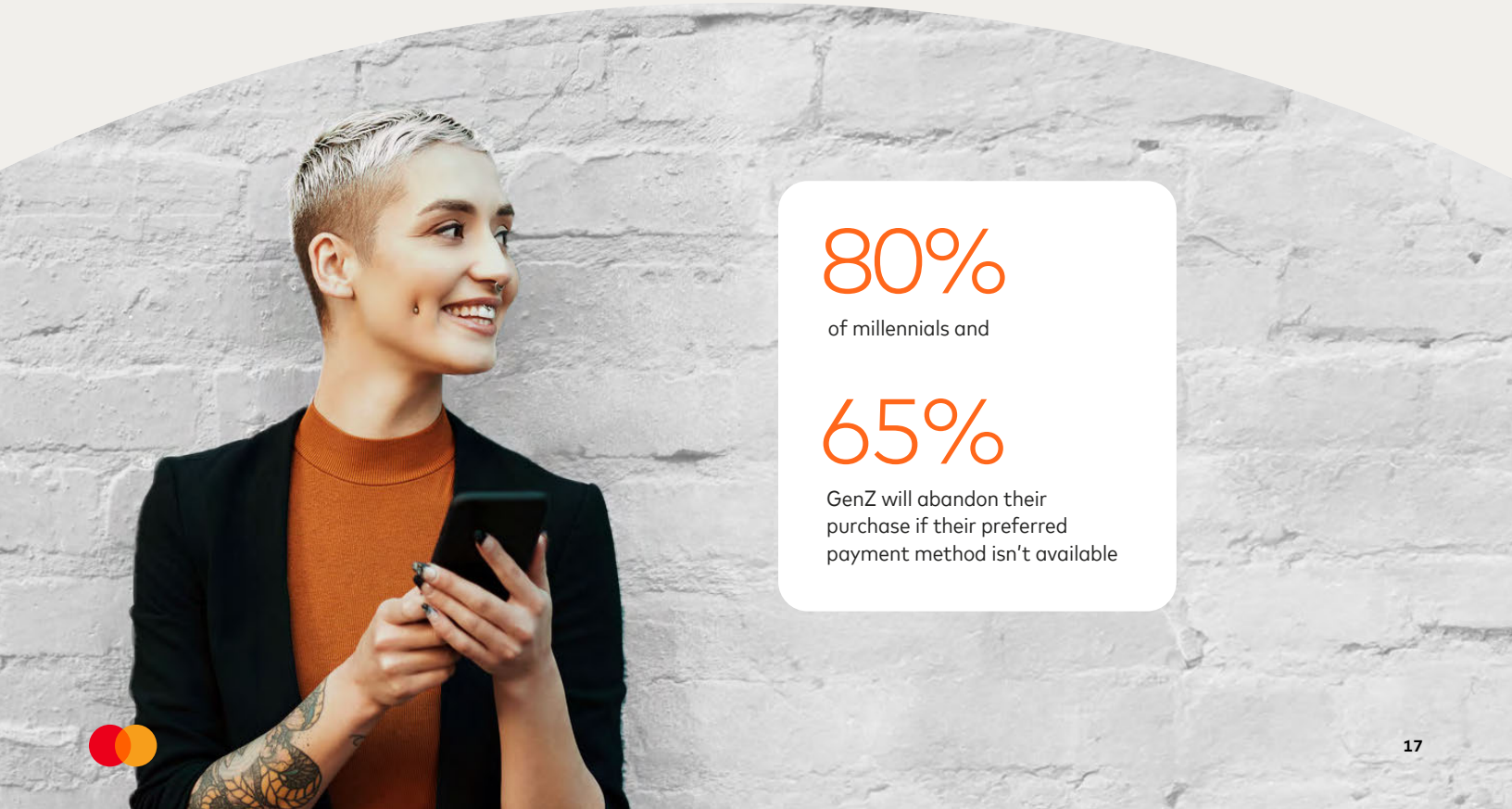
Customer experience

Today's customers expect seamless, frictionless interactions, especially regarding payments. A recent survey highlights that 80% of millennials and 65% of Gen Z customers will abandon their purchase if their preferred payment method is not available.[32]

This low tolerance for friction highlights the need for organizations in the payment ecosystem to balance security with a smooth customer experience when implementing fraud solutions. AI tools help them achieve this balance through improved accuracy, minimizing false positives and unnecessary transaction disruptions.

Operations

Beyond customer experience, AI and advanced analytics pose huge opportunities for business operations. Transaction data of a customer can help organizations create personalized experiences, tailoring products, services or unique offers to the customer's taste. On a larger scale, a network-wide analysis of transaction data can help businesses predict sales patterns that inform supply chain and manufacturing adjustments or marketing initiatives. These insights can help direct business strategies and prevent excess inventory or wasted resources.



80%

of millennials and

65%

GenZ will abandon their purchase if their preferred payment method isn't available

03

Protecting the future of AI through ethics and governance

While AI is integral to combating fraud effectively, ensuring it complies with ethical and governance frameworks is important — especially in the highly regulated financial sector.

AI governance

Regulations and compliance

Regulators stress the need for robust risk management with any technology. While individual regulator frameworks may apply across entities and jurisdictions, national governments are also creating frameworks and legislation to support the safe implementation of AI. Examples include the recently enacted European Union's AI Act, which is the world's first regulation of its kind.[33] The Act aims to regulate AI according to the risks it poses, with high-risk systems requiring compliance with strict requirements such as risk-mitigation systems, high-quality datasets, and human oversight.[34] Evidence of regulatory oversight is seen in other parts of the world, including the non-binding U.S. Blueprint for an AI Bill of Rights[35] and the United Kingdom's early-stage discussions of an AI Regulation Bill.[36] In major financial centers such as Singapore, the government has launched a National AI Strategy 2.0 with updated governance frameworks and guidelines.[37]

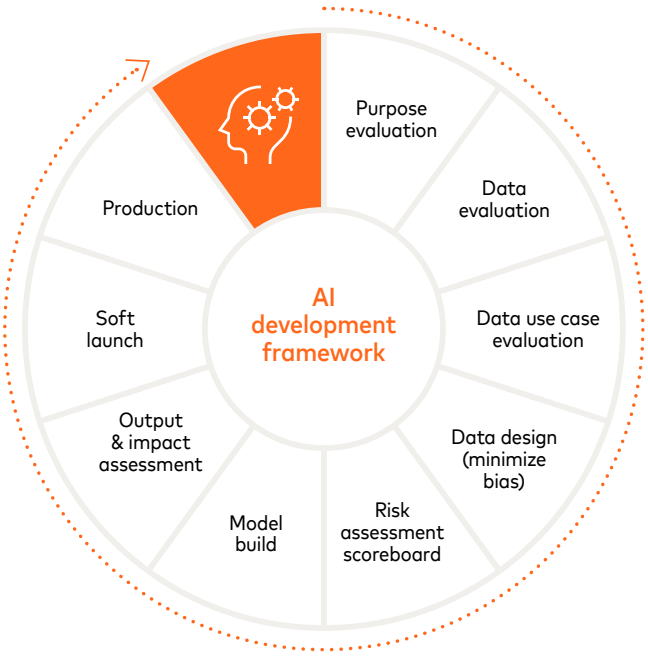
Partnering with AI solution providers that actively engage with global regulators and align with evolving regulations and governance frameworks helps businesses confidently deploy AI. This approach helps ensure organizations are meeting regulatory requirements at both macro and micro levels.

AI GOVERNANCE IN ACTION

Mastercard's AI governance framework

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

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



> *If it doesn't scale, it doesn't matter.*

Ed McLaughlin | President and CTO of Mastercard

PART THREE

Ethical AI

From accessibility to transparency

For AI to be ethical, it must be accessible, transparent and explainable. This means ensuring AI is easy to deploy, supported by comprehensive training and backed by sufficient and ongoing research and development.

Preventing bias

Transparency is crucial, as AI-driven decisions — such as credit scoring or loan approvals — must be explainable to ensure fairness and maintain regulatory compliance. Bias mitigation is a significant concern; without careful design and oversight, AI models can inadvertently reinforce existing biases in data, leading to unfair treatment of certain demographic groups. Additionally, accountability mechanisms are essential to mitigate errors or unintended consequences, ensuring institutions remain responsible for AI-driven outcomes.

Privacy by design

Ethical AI requires data security and privacy to be integrated into every stage of its development so that sensitive information is protected.

Consumer trust is also very important for ethical, responsible practices. Global survey data found that trust is the most important quality in banking, with respondents rating their bank's trustworthiness at approximately 4.2 index points out of 5.[38] The industry should prioritize transparency and privacy throughout all stages of AI implementation to keep this trust. Financial institutions should publicly share their data responsibility practices, such as a clear data bill of rights.[39]

PRIVACY PRACTICES IN ACTION

Mastercard's commitment to privacy

We believe personal information is exactly that — personal. Mastercard uses anonymized and aggregated transaction data, embedding privacy safeguards into all our products and services. We limit data use to what's necessary, seek ways to encrypt or de-identify personal information and make sure our products remain user-friendly. Rigorous standards protect data within Mastercard and across our partners and vendors.[40]

Using AI for good

Beyond securing the safety of the payments ecosystem and combating fraud responsibly and ethically, AI can contribute to broader social benefits — such as fostering inclusive growth, social impact projects and sustainability initiatives. Collaborations between academia, nonprofits and AI-focused initiatives are already tackling global issues and advancing these goals. For example, the United Nations World Food Programme uses AI and satellite imagery through its SKAI project to deliver real-time and actionable intelligence for disaster response.[41]

Financial inclusion

Financial inclusion is a critical area where AI can make a significant impact with 1.4 billion people worldwide remaining unbanked.[42] Even individuals with a bank account may be underbanked, meaning they don't have access to a full range of financial services such as credit, and rely on alternative financial services outside of the traditional banking system. AI offers promising use cases to bridge this gap, such as analyzing alternative data to assess creditworthiness for those without a formal credit history, helping millions to access loans.

AI FOR GOOD IN ACTION

Mastercard's Center for Inclusive Growth

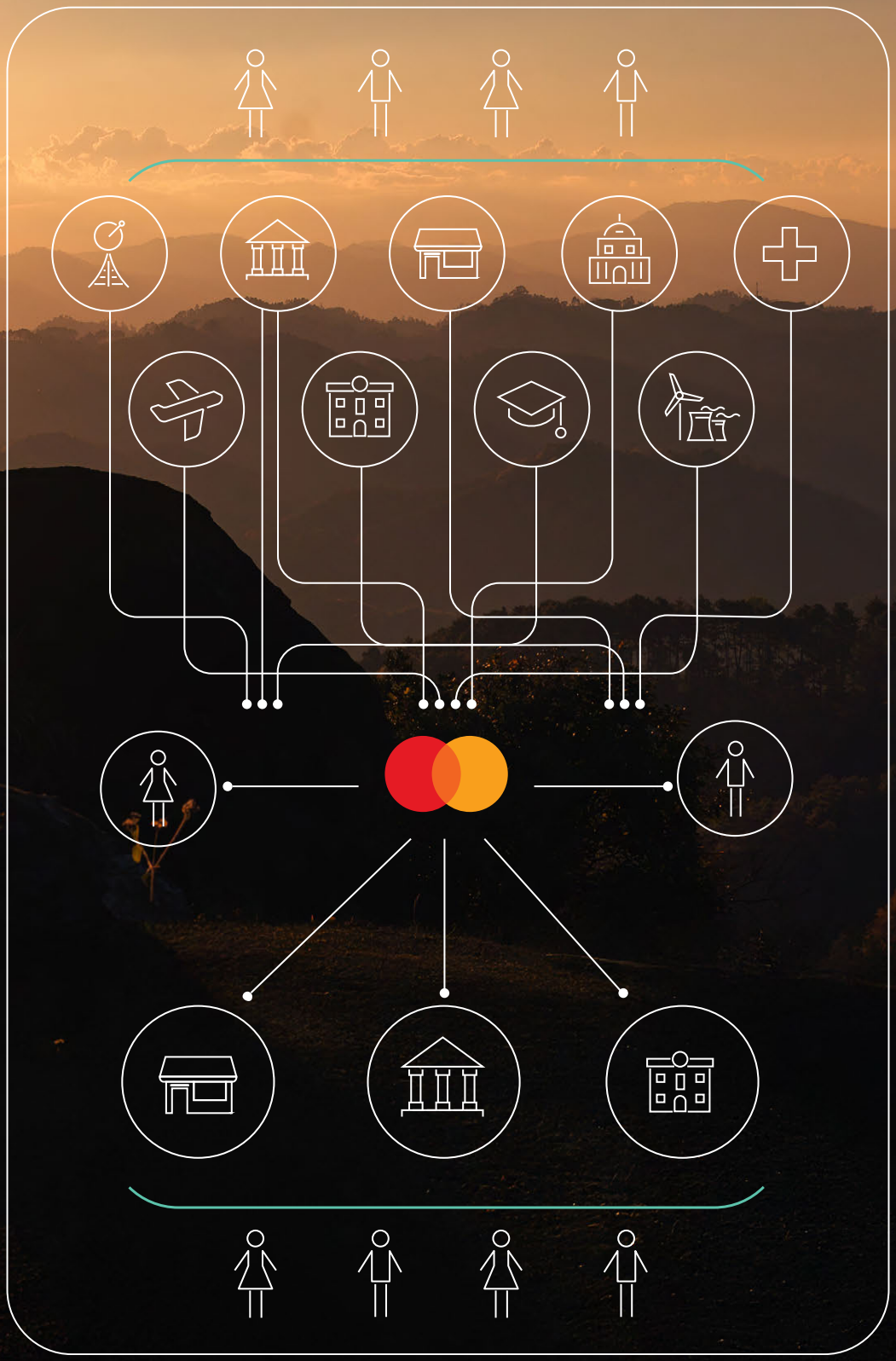
Mastercard's Center for Inclusive Growth has supported initiatives, such as FinRegLab and Women's World Banking, which use alternative data and machine learning to develop models that improve credit decision-making and promote financial inclusion for marginalized communities.[43]

center for inclusive growth

FinRegLab

Women's World Banking

A unique perspective



- Mastercard is at the center of the digital economy
- We're trusted by consumers and businesses
- We're uniquely positioned to protect against fraud and risk

A legacy of trust

Our strategic approach

For over 60 years, Mastercard has built a reputation for trust and carefully handling personal and private data. AI has been integral to our evolution, helping us secure the digital ecosystem from fraud, risk and cybersecurity challenges.

Our unique strategic approach sets us apart. We deliver AI-powered products and services across the digital ecosystem, with continuous investment in research and development through the AI Innovation Centre in India and the Mastercard Center for Advanced AI and Cyber Technology in Dubai.

Collaborating with governments and businesses worldwide, we help to develop processes and policies that uphold ethical standards. Additionally, we use AI to promote financial inclusion and societal benefits, empowering customers to solve their most pressing challenges with innovative, cutting-edge solutions.

What's next?

As the digital ecosystem expands and fraudsters adapt their methods to more innovative techniques, AI has moved from being a strategic advantage for the payments ecosystem to a necessity in combating fraud, enhancing security and maintaining trust. In this shifting landscape, organizations are compelled to adopt AI. Continued investment in technology development and close collaboration with governments and stakeholders are key to fully realizing AI's great potential and creating a safer digital world. However, to make meaningful strides in the fight against fraud, players across the ecosystem must trust global solution providers with their intelligence to build stronger, more unified defenses.

References

1. Nasdaq, Nasdaq releases first global financial crime report, measuring the scale and human impact of financial crime, January, 16, 2024
2. Juniper Research, Digital commerce transaction value to reach $20 trillion globally by 2027, September 21, 2022
3. Statista, Number of internet and social media users worldwide as of July 2024, September 20, 2024
4. International Monetary Fund, Stacking up financial inclusion gains in India, July 2021
5. McKinsey & Company, The rapid evolution of payments in Latin America, May 7, 2024
6. Juniper Research, Digital banking users to exceed 3.6 billion globally by 2024, as digital-only banks catalyze market, March 3, 2020
7. Mastercard, Data quality for accurate AI fraud and risk scores
8. Nasdaq, Nasdaq releases first global financial crime report, measuring the scale and human impact of financial crime, January, 16, 2024
9. Deloitte, Generative AI is expected to magnify the risk of deepfakes and other fraud in banking, May 29, 2024
10. Bank automation news, New study highlights tech trends and top priorities for banks in 2024 and 2025, June 3, 2024
11. IBM, X-Force Threat Intelligence Index 2024
12. Mastercard, The 2024 state of ransomware
13. The Record, Hackers are targeting Asian bank accounts using stolen facial recognition data, February 15, 2024
14. LexisNexis, The LexisNexis risk solutions cybercrime report
15. NILSON, Issue 1254, December 2023, December 18, 2023
16. Mastercard, FraudWatch: the 'how to' of preventing BIN attacks, 2023
17. Mastercard, What is synthetic identity fraud and how does synthetic identity theft work?
18. Security, Synthetic identity fraud fastest growing financial crime in US, August 18, 2023
19. Forbes, Synthetic identities: the Darker Side of Generative AI, May 29, 2024
20. Mastercard, What is synthetic identity fraud and how does synthetic identity theft work?
21. NILSON, Issue 1254, December 2023, December 18, 2023
22. Finextra, Three types of merchant fraud: a guide for merchant acquirers, November 21, 2017
23. Mastercard, A2A payment trends, risks and fraud solutions
24. Federal Trade Commission, "Love stinks" - when a scammer is involved, February 13, 2024
25. U.S. Senator Richard Blumenthal, Blumenthal, Warren & Walters introduce legislation to protect consumers from payment scams, August 2, 2024
26. BBC, Banks must refund fraud up to 85,000 in five days, September 25, 2024
27. Mastercard, AI in financial services: from data fragmentation to data orchestration
28. US Department of the Treasury, Managing artificial intelligence-specific cybersecurity risks in the financial services sector, March 2024
29. Mastercard, Inside the algorithm: how genAI and graph technology are cracking down on card sharks
30. Forbes, Six key ways GenAI can enhance your fraud management strategy, September 26, 2024
31. US Department of the Treasury, Managing artificial intelligence-specific cybersecurity risks in the financial services sector, March 2024
32. Forbes, 4 trends in gen z and millennial payment preferences for e-commerce, May 23, 2023
33. European Parliament, EU AI act: first regulation on artificial intelligence, June 8, 2023
34. European Commission, AI Act enters into force, August 1, 2024
35. The White House, Blueprint for an AI bill of rights
36. The UK Parliament, Artificial intelligence (Regulation) bill (HL): HL Bill 11 of 2023-24, March 18, 2024
37. Smart Nation Singapore, National AI Strategy
38. Statista, Bank customer trust levels worldwide in 2024, by country, April 18, 2024
39. Mastercard, Data and tech responsibility
40. Mastercard, Explore privacy at Mastercard
41. UN World Food Programme, SKAI project overview
42. World Bank, COVID-19 boosted the adoption of digital financial services, July 21, 2022
43. Financial Times, It's time for industry leaders to start using AI for good; here's how