OCTOBER 2023

THE UPDATE

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

ARTIFICIAL INTELLIGENCE

Generative AI is knocking at the door of the financial world. **Do we let it in?**

INSIDE THIS EDITION

Artificial Intelligence + Identity + Cyber + Risk & Resiliency

PLUS

WIN with Risk X

Foreword

Ajay Bhalla
President of Cyber
& Intelligence at Mastercard

Welcome to the first edition of The Update.

In today's world, where the power of technology is harnessed for both good and bad, the need for cybersecurity and trusted solutions extends ever deeper into every corner of our global digital ecosystem. But at the same time, the opportunities to harness this innovation, to grow business, enhance customer experience and become more effective are just as crucial.

With new technologies like generative AI, we stand at the precipice of yet another transformative leap. This groundbreaking technology may be the most important tech of our time, heralding a new era of commerce and innovation, reshaping our industries.

Estimates suggest that AI could contribute as much as $15.7 trillion to the global economy by 2030.

It's with this backdrop that we set out to create The Update. We have brought together a series of insightful features and opinions from Mastercard's subject matter experts, offering guidance on how to navigate the new normal of modern life being intertwined with the digital realm.

In this very first edition we cover a wide range of issues and topics, from how AI is central to the war on scams to a horizon view of what's next for digital banking. With expert insights and actionable guidance, we dissect complex issues into easily digestible pieces, with the aim of keeping you informed.

As always, I want to offer a heartfelt thank you for being our partners. Mastercard may sit at the centre of our digital ecosystem, but it's only with your partnership that we can protect it for all.

I do hope you enjoy reading this first edition. If you have thoughts or opinions that you'd like to share back with me, I'd love to hear them.

With thanks,

Ajay Bhalla

Contents

EDITORIAL

04 Shaping AI to protect our digital futures >

ARTIFICIAL INTELLIGENCE

08 Artificial intelligence is driving security in the payments ecosystem >

10 Mastercard Gateway and Brighterion: The right partnership matters >

12 Enlisting AI in the fight against money laundering >

15 Generative AI is knocking at the door of the financial world. Do we let it in? >

17 The AI imperative: Overcoming obstacles to curb surging digital payment fraud >

19 Mastercard's new global AI Centre will unlock AI's potentiald >

IDENTITY

21 The road to data excellence >

24 Industry best practices for e-commerce fraud detection >

26 Supercharge your KYC with digital identity verification >

CYBER

29 Mastercard brings its latest AI capabilities to the fight against payment scams >

32 Keep it simple: The impact of DORA and NIS2 on third-party risk management >

35 What lies ahead: The future of digital banking >

38 How to identify and manage VASP counterparty risk >

41 The future of cyber risk management >

RISK & RESILIENCY

45 Building resilience in payments >

47 How telecom providers stay ahead of third-party risk >

51 Companies can no longer ignore ESG risks >

Shaping AI to protect our digital futures

Ajay Bhalla
President of Cyber & Intelligence at Mastercard

Alex Pentland
Professor at MIT and Director of Connection Science

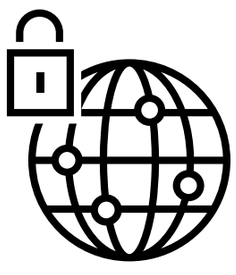
The growing attention paid to generative AI tools such as ChatGPT has captured our collective imagination. The versatility of this technology has enabled professionals in every sector to envision how AI can alter human interactions with the digital world. From content creation to more complex tasks like fraud prevention, the capabilities for generative AI seem endless. However, it won't have a revolutionary impact — for example, to the same effect that AI has had on personalised video streaming over traditional TV — unless it is populated with the data needed to truly bring it to life. Without up-to-date, high-quality data, generative AI will not sustain its status as a game changer that can reinvent the digital experience for businesses and consumers.

Generative AI's success requires fixing our data ecology

Providing AI with the data it needs will require us to rethink how our data is shared to meet the compliance and copyrighting needs of data owners. Data environments have remained relatively untouched in the past decade, since the introduction of cloud storage systems. Data ownership and sourcing rights have been a pressure point, with organisations needing faster access to data while still complying with regulatory guardrails.

In general, data ecology has historically been light in touch. However, the arrival of technology like GPT-4 is motivating data owners to incorporate better data sourcing and governance procedures, such as data tagging. This is not a bad thing and has led to the emergence of innovative data governance models, such as data cooperatives, which promote the idea that organisations and individuals can collectively control and benefit from their data. In their simplest form, these are just repositories of training data where ownership rights and attributes such as collection date and quality assurance are clearly marked. An example of this is the MIT Media Lab's Data Provenance Initiative.

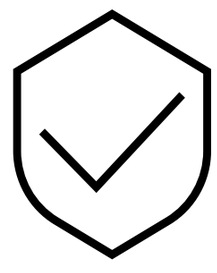
More proactive are data exchanges like Gaia-X, which aim to provide data owners (licensors) with the ability to provide revokable and specific rights to organisations to use their data for the training of models.



Generative AI must deliver value without loss of IP or competitive advantage

Feeding generative AI models the high-quality data they need comes with a risk to customer privacy, though, and AI's future success hinges on trust and our collective ability to create systems that inspire faith from consumers. Avoiding these privacy issues will require trusted networks (e.g., legal and data architectures like the Mastercard network), federated AI and TEEs (Trusted Execution Environments). The goal would be to enable data to be used securely and privately, so that AI models can offer contextually relevant answers, but without revealing private aspects of the data-owning community or its members. Privacy-preserving methods like these allow community members to see real value without the risk of data leakage.

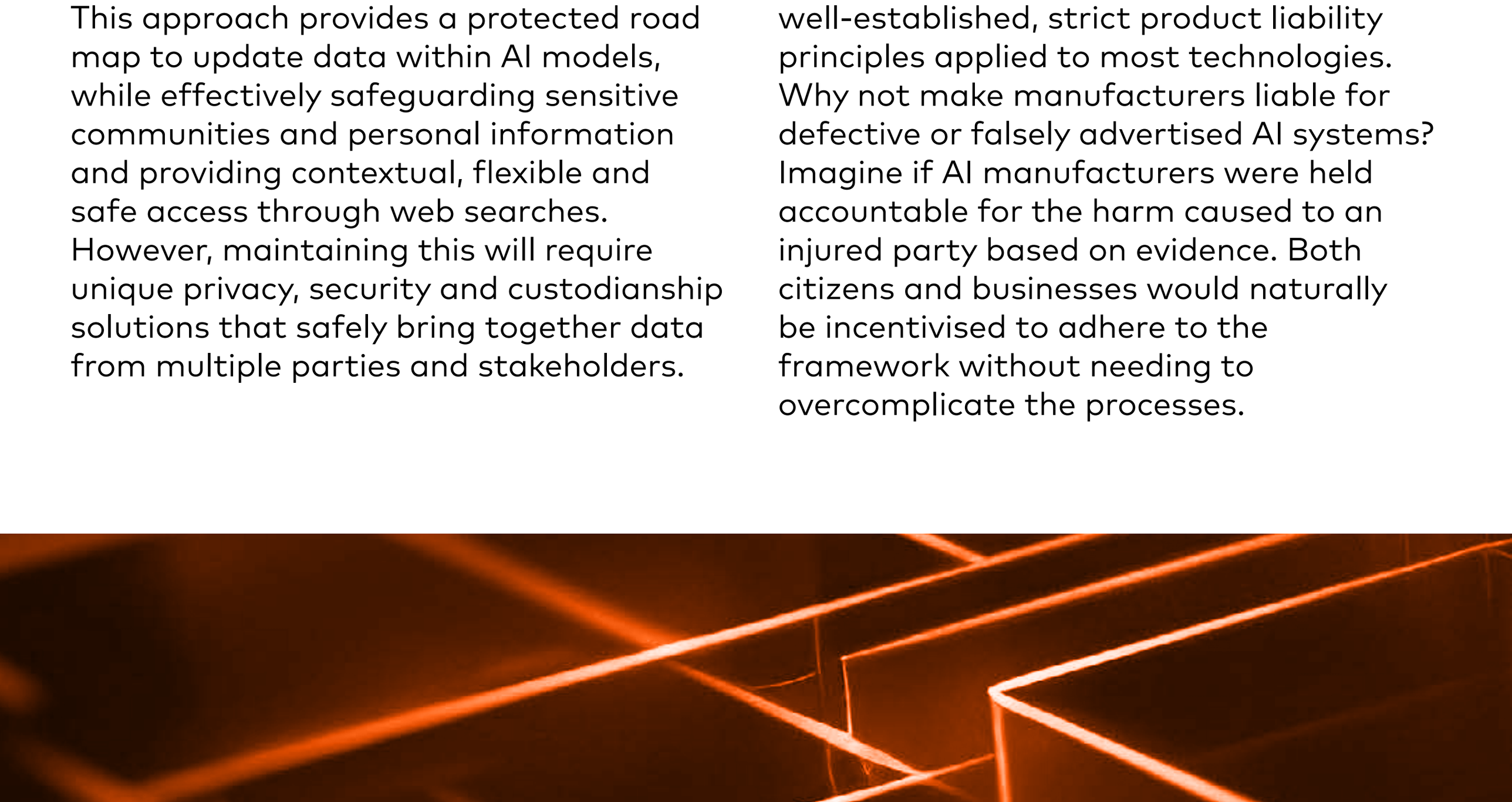
This approach provides a protected road map to update data within AI models, while effectively safeguarding sensitive communities and personal information and providing contextual, flexible and safe access through web searches. However, maintaining this will require unique privacy, security and custodianship solutions that safely bring together data from multiple parties and stakeholders.



How to ensure the safety and performance of AI

Both EU and U.S. government guidelines stress the need to protect consumers without hampering AI innovation. However, elements of the proposed EU regulation on AI may be unachievable — for example, the requirements on high-risk AI systems: 'Training, validation and testing data sets shall be relevant, representative, free of errors and complete'. Virtually no dataset is likely to be complete, and some degree of error is always present. Imposing these static rules irrespective of context misunderstands how AI is developed and not only fails to protect consumers but also deters desirable innovation.

Instead, we would advocate for more flexible legal frameworks that introduce incentives for AI creators to release safe products. Today we already have well-established, strict product liability principles applied to most technologies. Why not make manufacturers liable for defective or falsely advertised AI systems? Imagine if AI manufacturers were held accountable for the harm caused to an injured party based on evidence. Both citizens and businesses would naturally be incentivised to adhere to the framework without needing to overcomplicate the processes.



To ensure fairness, the process would need to outline clearly when a defective AI system caused harm by creating a baseline (a human or another AI) to compare with. This is where auditing AI behaviour becomes important, because it lets us know the degree to which a model's prediction gave rise to a certain harm. AI manufacturers must be required to maintain anonymised records of input data and model outputs that can be analysed in any legal process.

Auditing for certification is already part of the proposed EU AI regulations, and in Singapore they have released AI Verify, an AI auditing and testing framework for companies based on internationally accepted AI governance principles. AI Verify does not define ethical standards but rather enables developers and owners to demonstrate their claims about the performance of their AI systems.

While still in a pilot phase, Singapore's efforts represent further development of the debate on AI governance and regulation, and are a response to the growing demand for trustworthy AI systems and interoperability in global AI regulatory frameworks.

As AI becomes ever more ingrained in our lives, regulators seeking to protect consumers while also promoting innovation must understand that there is no one-size-fits-all global solution. As is seen with electricity, cars, bridges, highways and so on, rigid regulation of new technologies has always been a poor general approach to making technology safe. Void of any flexibility, fixed regulation fails to anticipate new applications and capabilities, and restricts only local developers who then can't compete in a global market. Instead, implementing a more flexible auditing regulatory framework will both narrow the scope of records for error assessments and make it easier to appeal an automated decision. The reason that Singapore and the EU have made auditing central to AI regulation is to ensure ethical performance and regulatory compliance while avoiding bias and ensuring provenance.

Finally, this is a learning process; we shouldn't expect globally applicable solutions but instead a focus on where the benefit of AI can be clearly demonstrated, and maintain a level of transparency that opens the door for people to engage positively.

ARTIFICIAL INTELLIGENCE

08 Artificial intelligence is driving security in the payments ecosystem >

10 Mastercard Gateway and Brighterion: The right partnership matters >

12 Enlisting AI in the fight against money laundering >

15 Generative AI is knocking at the door of the financial world. Do we let it in? >

17 The AI imperative: Overcoming obstacles to curb surging digital payment fraud >

19 Mastercard's new global AI Centre will unlock AI's potential >

Artificial intelligence is driving security in the payments ecosystem

The key to the future of fraud protection is keeping personal information personal

Rohit Chauhan
Executive Vice President,
Artificial Intelligence

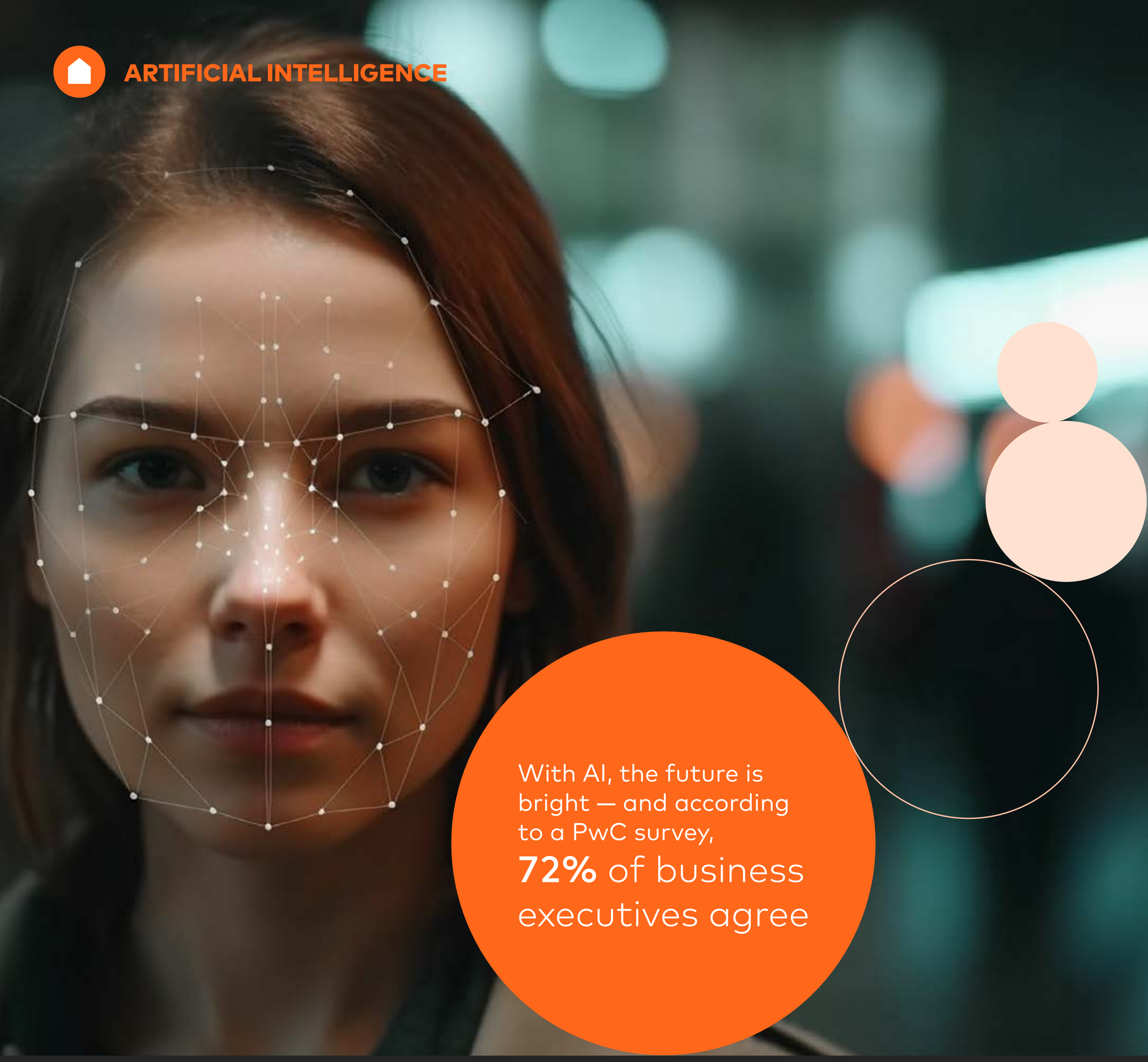
Whether driving news cycles or conversations around the boardroom (and dinner) table, artificial intelligence is on everyone's mind today. Yet even though the technology is having 'a moment', AI is not new.

For more than a decade, Mastercard has been harnessing the power of AI to fuel our products and solutions, enlighten our customers and drive innovation. We have long pioneered the development of groundbreaking AI solutions, which protect our payments ecosystem across the life cycle of a payment transaction.

In short, AI is critical to the solutions we provide our customers. Our global identity verification solutions leverage machine learning to determine whether people are who they say they are, building trust on both sides of a digital interaction. Baffin Bay Networks, which Mastercard recently acquired, provides a cloud-based solution that uses the latest in AI technology to automatically filter and counteract malicious internet traffic. And our Safety Net technology leverages AI and machine learning to detect large-scale fraud attacks quicker and more accurately than ever before.

Artificial intelligence allows us to protect the 125 billion transactions we switch on our network every year at speed and scale. By applying thousands of data points, our sophisticated AI engine helps banks approve more genuine transactions and prevent fraud. In fact, our AI-powered solutions have saved $35 billion in fraud in the past three years alone.

Artificial intelligence allows us to protect the **125 billion** transactions we switch on our network every year at speed and scale.



With AI, the future is bright — and according to a PwC survey, **72%** of business executives agree

Fighting fraud around the world

Earlier this year, Mastercard announced a partnership with Network International, the leading enabler of digital commerce in the Middle East and Africa, to address fraud, declines and charge-backs, and to reduce costs and risks for acquirers. Leveraging Mastercard's Brighterion AI technology, Network International will provide transaction fraud screening and merchant monitoring to its customers across the region.

Brighterion creates AI models that identify behaviour indicative of transaction fraud. Brighterion's Transaction Fraud Monitoring intercepts fraud at the pre-authorisation stage, before an acquirer submits the transaction authorisation to the payment network. Because the solution is trained on the most sophisticated fraud attempts around the world, protection and accuracy are high, enabling a secure ecosystem with an optimal experience for end cardholders and merchants.

Fuelling the industry and the future

At Mastercard, we think of AI like electricity: powering our society, enlightening our communities and driving progress. That's why we use it everywhere we can, while understanding and minimising the risks. We believe innovations in AI must be done right, and with great care. This means ensuring that the right controls, ethics and governance are in place. To that end, we have embedded strong controls into all our touch points with AI.

Our data responsibility principles ensure that 'personal information' is just that — personal — and that it remains that way.

Mastercard continues to invest in both the people and the technology to fuel AI. With AI, the future is bright — and according to a PwC survey, 72% of business executives agree. Like Mastercard, they see AI as a business advantage that will play a fundamental role across the industry for years to come.

Mastercard Gateway and Brighterion: The right partnership matters

Gateway orchestration and advanced fraud technology solutions power commerce to help solve today's growing business challenges

Maria Parpou
Executive Vice President, Payment Gateway Services

Sudir Jha
Executive Vice President, Head of Brighterion

In today's dynamic payment landscape, commerce has shifted dramatically to being digital by default. With this new digital payment evolution, our two services, Mastercard Gateway and Brighterion, have reflected on how we support our customers in this complicated space.

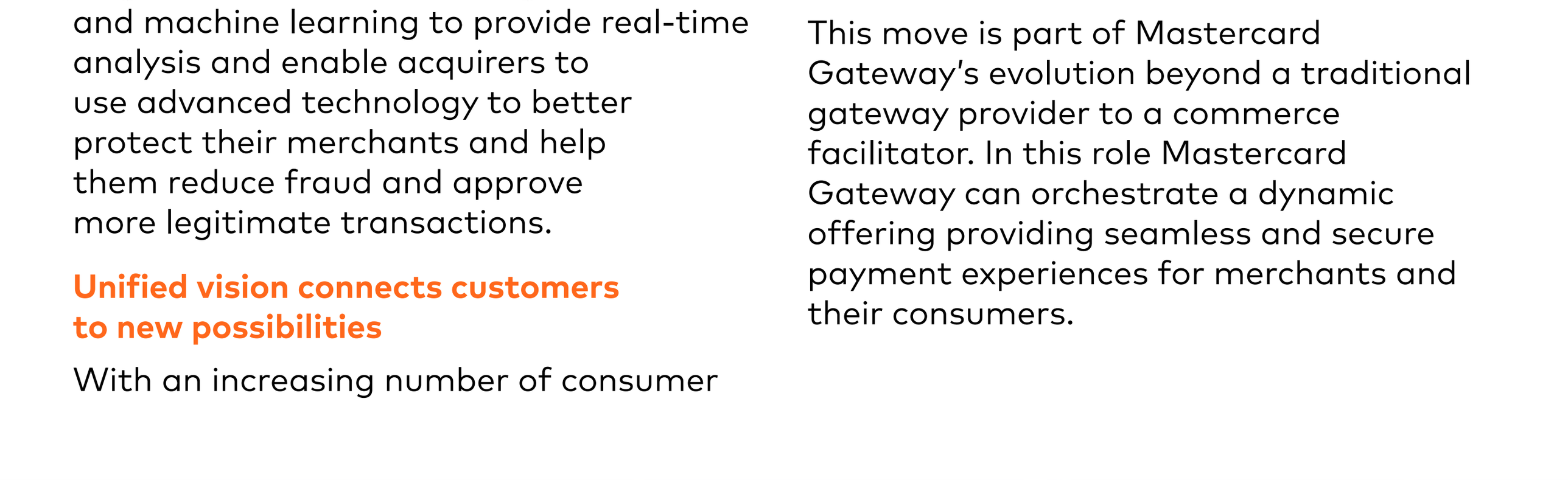
Mastercard Gateway powers commerce for financial partners, ISVs and merchants through a single touch point to accept payments globally and expand into new markets. Together with Brighterion, we have launched an anti-fraud integration: Transaction Risk Management powered by Brighterion. This service leverages Brighterion's artificial intelligence (AI) and machine learning to provide real-time analysis and enable acquirers to use advanced technology to better protect their merchants and help them reduce fraud and approve more legitimate transactions.

Unified vision connects customers to new possibilities

With an increasing number of consumer touch points, it's become harder for acquirers and merchants to get a complete view of their consumers' behavioural patterns. This leads to a fragmented approach to fraud prevention and may cause vulnerabilities. To solve this, Brighterion and Mastercard Gateway have integrated their solutions to secure the payment process and better meet customers' continuously evolving needs.

The Brighterion integration within Mastercard Gateway can now deliver a unified ecosystem enabling acquirers to proactively detect, prevent and mitigate fraudulent activities, ensuring enhanced security for both acquiring customers and their enterprise merchants.

This move is part of Mastercard Gateway's evolution beyond a traditional gateway provider to a commerce facilitator. In this role Mastercard Gateway can orchestrate a dynamic offering providing seamless and secure payment experiences for merchants and their consumers.



How Mastercard Gateway and Transaction Risk Management powered by Brighterion work

Each transaction sent by Mastercard Gateway to Brighterion is evaluated within its perimeter in two paths: the AI model and the rules set by the customer. The AI model checks against multiple transaction indicators and compares them with patterns identified in historical customer and Mastercard data as correlated with fraudulent use. The model is monitored to evaluate when retraining is necessary.

The second framework established by Mastercard Gateway and Brighterion assesses the transaction with a rules-management tool. Customers can use a variety of rules within the supported templates, as well as establish their own based on business specifics.

After the assessment, each transaction is assigned a numerical score that indicates the level of risk associated with the transaction.

The score, rules and AI indicators together provide a complete picture of the fraud screening process, which is essentially done on a real-time basis.

1

Customer sets the rules and thresholds within the Brighterion User Interface when establishing the solution.

2

When a transaction is being initiated by a cardholder, relevant information is transmitted by Mastercard Gateway to Brighterion.

3

Brighterion evaluates the transaction data using models and rules and generates a real-time response of Accept or Reject.

4

‘Accept’: The Gateway actions the payment accordingly and sends the transaction to the issuer.

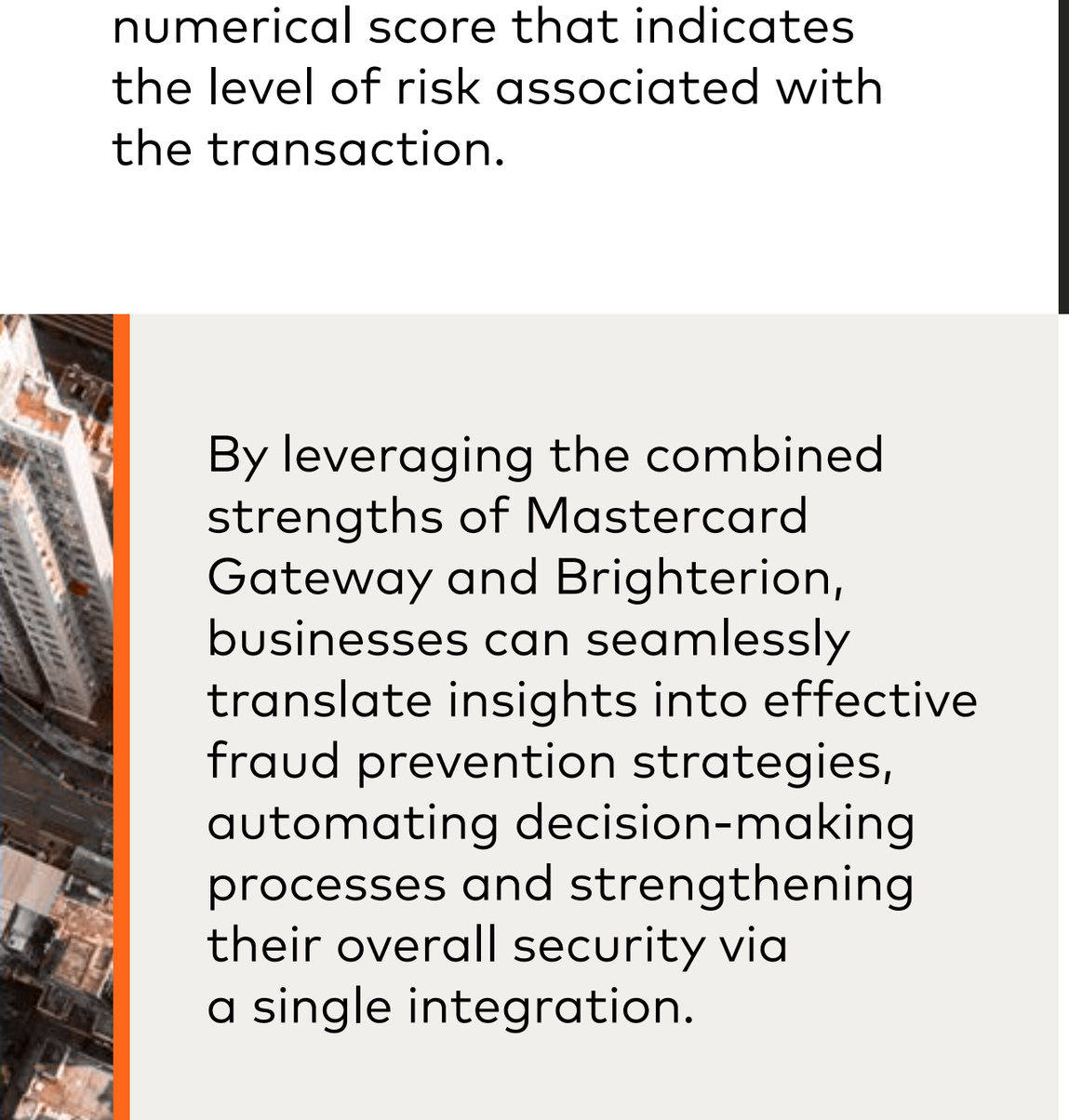
5

‘Reject’: The Gateway actions the payment accordingly and sends a decline response to the customer.

6

The transaction score and rules are provided to the Gateway in real time and are viewable via the portals.

By leveraging the combined strengths of Mastercard Gateway and Brighterion, businesses can seamlessly translate insights into effective fraud prevention strategies, automating decision-making processes and strengthening their overall security via a single integration.



A new horizon for customer experience, driving success

The collaboration between Mastercard Gateway and Brighterion shows how customers can leverage the expertise of Mastercard across a diverse skill set to innovate their payment strategy with an end-to-end service that focuses not just on the technology but also on the customer service and experience.

We are proud to offer this integrated solution and look forward to empowering organisations with the tools and insights they need to stay one step ahead in the battle against fraud.

Enlisting AI in the fight against money laundering

Jonathan Anastasia
Executive Vice President, Crypto and Security Innovation

$5 billion
in fines for breaches and AML infraction in 2022, a 50% spike from the previous year

Criminals across the globe launder $2 trillion every year.[1] And whether they're street-level drug dealers or white-collar embezzlers, each one of these criminals needs to make their illegal funds look legitimate. The methods they use to hide their earnings are almost as varied as the crimes themselves, so thwarting them is an extremely complex task.

The most reliable way to prevent money laundering is to evaluate every deposit or payment customers initiate and to escalate the most suspicious transactions for further investigation. To scale the process, most banks rely on automated monitoring software. But these systems tend to be rules-based and inaccurate, powered by datasets that are neither broad nor detailed nor up to date enough to represent the full scope of money-laundering schemes. High false-positive rates — 98% of transaction monitoring alerts are false alarms[2] — can be an especially costly drawback, since they monopolise resources while delivering zero value toward the detection of money laundering.

This is where harnessing the power of artificial intelligence (AI) can be a game changer. Through daily monitoring of suspicious money-laundering activity across a network and using predictive AI technology and machine learning, financial institutions can ensure improved accuracy in detection of potential money laundering.

Understanding money laundering at the account level

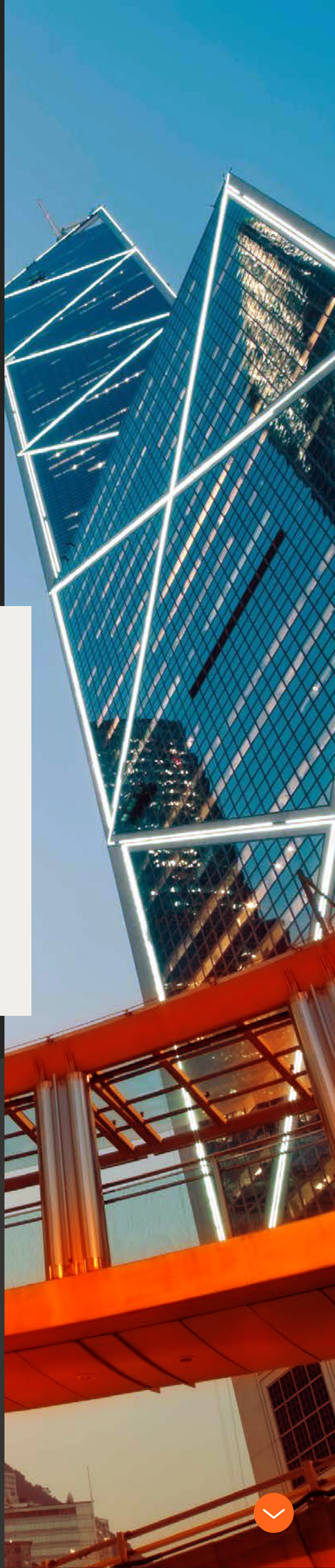
As with many other types of financial misconduct, banks are a key barrier against money laundering, and their prevention strategies are held to high standards. Anti-money laundering (AML) regulations vary from country to country, but most require financial institutions to record every transaction, train staff to recognise and report suspicious activity, verify Know Your Customer (KYC) information and report large deposits.

Unfortunately, these measures aren't enough, and the problem is only getting worse. **Financial institutions were fined $5 billion for breaches and AML infractions in 2022, a 50% spike from the previous year.**[3] Criminals are continually adopting new and more sophisticated tactics to disguise their ill-gotten gains, and AML methods must evolve to keep up.

AML Account Risk, a new AI-powered transaction monitoring system from Mastercard, can help banks gain a deeper understanding of their money-laundering risk at the cardholder level.

The solution monitors suspicious activity across the Mastercard network — scanning billions of card-based transactions each year at ATMs, brick-and-mortar businesses and e-commerce sites around the world. It then applies Mastercard proprietary AI from this broad, network-wide view to highlight potential financial crime at the account level.

By analysing 14 high-risk parameters, AML Account Risk's AI technology recognises patterns indicative of money laundering, assigning each account a risk score based on its activity over time. If the score exceeds a certain threshold, the account is immediately flagged and the bank receives an automated notification. Arriving in near real time, these notifications call attention to higher-risk accounts that might slip past a bank's filters, helping financial institutions to take quick action.



Analysts can check the list of flagged accounts and their suspicious transactions via a web-based dashboard on Mastercard Connect. They can visit linked pages that focus on each account, with charts showing amounts spent and received, number of cross-border transactions, types of goods or services traded and merchants patronised. These visualisations can expose recent changes in behaviour, such as sudden surges in transaction volume or frequency.

To help banks triage their investigations, the dashboard can also rank accounts by other factors, including age and fastest increase in risk score. Banks can use the dashboard data independently or incorporate it into their existing AML protocols.

AML Account Risk assists financial institutions in detecting card-based money laundering more efficiently.

AML Account Risk augments financial institutions' existing card-based AML compliance processes, assisting with accurate identification and prioritisation of potential money-laundering accounts at PAN level.

'Through daily monitoring of suspicious activity across the Mastercard network, AML Account Risk can provide deeper insight into money-laundering risk.

That helps banks boost their operational efficiencies and safeguard their reputations'.

Improving detection and compliance

By enhancing their AML processes with advanced AI tools, banks can identify more illicit transactional trends. With better accuracy and fewer false positives, AML Account Risk's notification system allows banks to concentrate labour and resources on meaningful alerts. As part of an effective AML strategy, this industry-leading technology helps improve compliance and reduce the risk of penalties — protecting brand value and reducing financial crime worldwide.

Generative AI is knocking at the door of the financial world. Do we let it in?

Nitendra Rajput
Senior Vice President and Head of AI

Imagine a person walking barefoot in a desert. By analysing the size of the footprint, one can infer a number of attributes. The distance between footprints, for example, can indicate the person's height, as longer strides typically mean a taller person. Just by looking at a footprint, we can learn so much. Digital footprints provide similar insights, only they are here to stay and will not disappear with a gust of wind.

Generative AI may be the most important technology of our time, heralding a new era of commerce and innovation and promising to transform customer experiences, enable personalised interactions and reshape industries. Generative AI can 'generate' a richer profile about a customer from their digital footprints. If we expand our view to the billions of digital footprints all around, then we can generate profiles for products, organisations and many entities of interest to businesses.

Tectonic shifts are often the result of a confluence of several strong independent trends. In the case of generative AI in finance, the first trend has been the past decade of the financial world, where the number of non-cash transactions will now cross 1.3 trillion in 2023.[4] Next is the increase in computing infrastructure that powers the underlying AI algorithms. Using the volume of data that is now available and the technology that can manage this volume, generative AI algorithms have arrived at an opportune time. This is enabling new use cases, enhancing operational efficiency and improving productivity, thus changing the financial services landscape at tremendous speed.

It is estimated that generative AI could add the equivalent of **$2.6 trillion** to **$4.4 trillion** each year

At the same time, the ability to generate realistic content can be used for ill-gotten gains. Generative AI has the ability to create personalised phishing attacks that can better mimic authentic scenarios to be used for social engineering fraud scams. These sophisticated attacks can pose a significant challenge for organisations and individuals. AI also has the potential to drive powerful innovation to combat fraud and increase access to financial services — at scale and speed.

While generative AI will change the threat landscape, it also holds the promise to solve significantly difficult and challenging problems in the financial world. One such problem is that fraud patterns keep evolving continually over time. As we all know, data holds the key to the power of AI; however, when new fraud patterns emerge, AI algorithms must wait to have this data before they can be effective at preventing these new kinds of fraud. Generative AI is now being used to synthetically generate new fraud data on which AI models can learn to catch fraud patterns that otherwise would have escaped the lens.

Similarly, the ability to generate rich insights about the customer will help an organisation identify suspicious activities that do not match the customer profile. Some systems have already demonstrated the potential to auto-service customers and employees by providing them with specific and personalised information to solve the problem at hand, as opposed to having to navigate through a 500-page manual. Such automation can help in improving financial crime solutions efficiency, without having to increase manpower. The list of such use cases is endless, and we are still scratching the surface in terms of the potential!

No wonder the economic potential of generative AI is huge. It is estimated that generative AI could add the equivalent of $2.6 trillion to $4.4 trillion annually. Banking is among the industries that could see the biggest impact.[5] The fivefold increase in efficiency can be thought of as a new car that can drive five times faster than the ones we see on the road. To ensure that the roads are still safe, new rules will need to be made.

Similarly, generative AI solutions need to have the appropriate guardrails. Consumers are increasingly demanding privacy, transparency and accountability from organisations when it comes to how they handle data. Guardrails need to exist at multiple levels, starting with safeguards around data. Organisations will need to ensure that data privacy, data ownership and data sharing are in compliance with the local regulations of the region. These regulations are evolving, with many proposals in discussion globally.

At Mastercard, we have a robust AI governance framework that is grounded in our data responsibility principles. Anytime our teams want to use AI, the use case goes through our governance framework to ensure it is aligned with our data principles. To implement AI responsibly, organisations need a robust AI governance framework.[6] This will serve as a backbone to delivering efficient solutions to customers, while doing right by them.

These are extremely exciting times as AI unlocks new opportunities for us all. Technology and business are evolving and helping each other grow faster than ever. While there are ongoing discussions about generative AI technology, the financial world is often the first to ride a new technology wave, and this wave is too big to be missed.

The AI imperative: Overcoming obstacles to curb surging digital payment fraud

Amyn Dhala
Vice President,
AI Product Development

$32 billion
in global card fraud losses in 2021

A recent survey conducted by Mastercard and Fintech Nexus polled 100 financial institutions worldwide to gauge perspectives on leveraging artificial intelligence (AI) to combat fraud.

The results, published in the new AI Perspectives: Transaction Fraud 2023 report[7] — and summarised in this article with the assistance of generative AI — reveal strong interest in AI, but also barriers to adoption. As new payment types proliferate, anonymised transactions become increasingly ripe for criminal abuse. While AI offers hope for fighting back against fraud, ongoing implementation hurdles continue to hinder its real-world impact.

The report makes one thing clear: Financial institutions are embracing AI as a tool to improve fraud detection and prevention. Nearly half already use it, and 93% plan to invest more over the next two to five years. However, 47% still rely on rules-based systems, versus just 37% using AI. This disparity is striking, given AI's widely touted capabilities.

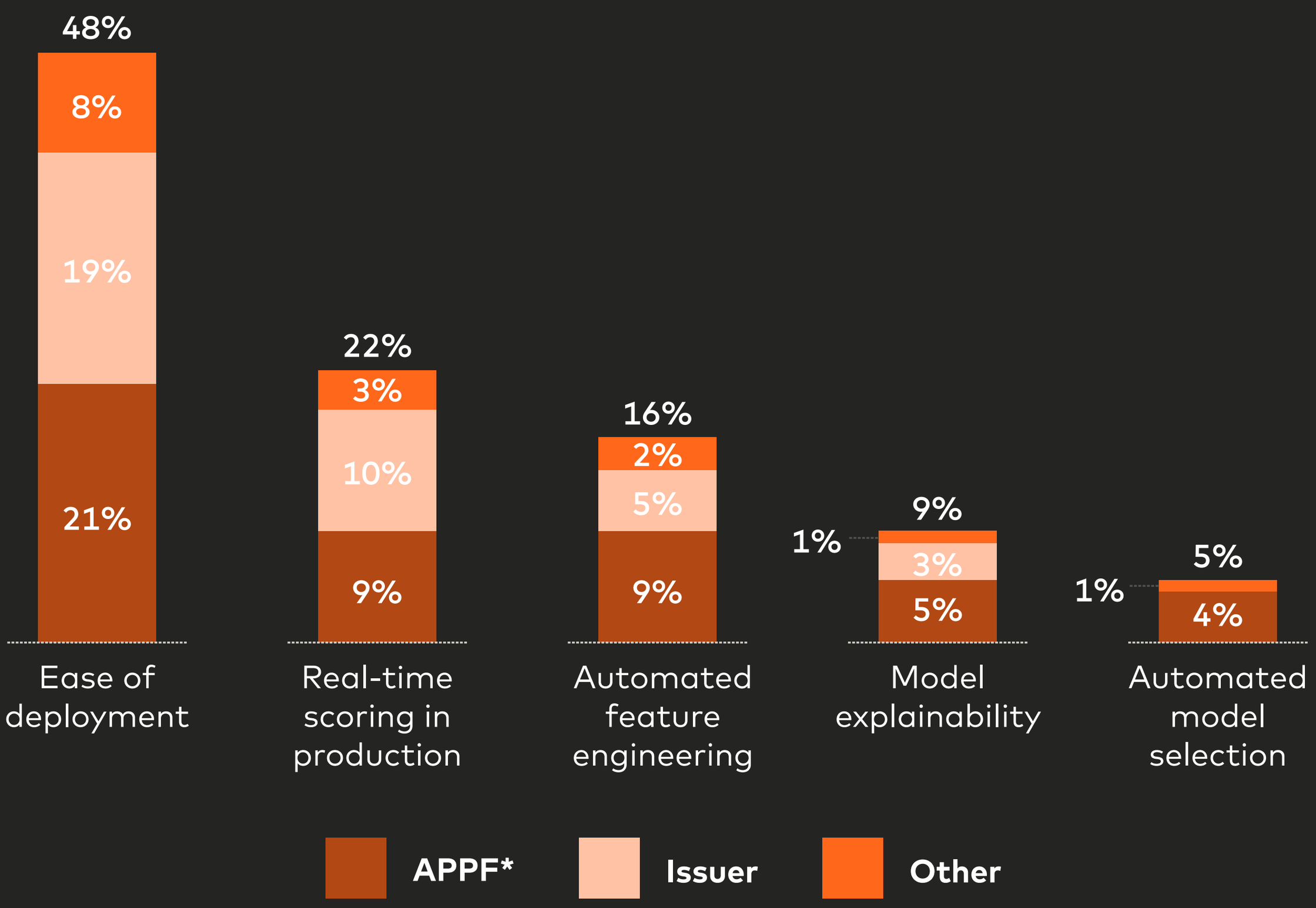
> Sixty-one percent of respondents flagged social engineering and authorised payment scams as the top A2A fraud threats. These types of scams directly manipulate human trust, tricking victims into willingly sending money to criminals. Though recipients quickly disappear, draining and then ditching associated accounts, banks may remain liable for massive losses. Hence, **65% believe AI can detect subtle anomalies and raise red flags**, signalling scams before they strike and succeed. That is, if systems are trained to spot anomalies that rigid rules miss.

AI and account-to-account payment fraud

The top driver for AI is enhanced fraud catch rates. According to the Nilson Report, global card fraud losses reached $32 billion in 2021, so it's obvious why 63% want better detection. As digital wallets and account-to-account (A2A) payments like P2P surge, anonymised transactions are vulnerable to fraud. AI's pattern recognition capabilities provide a ray of hope.

But what impedes real-world adoption and impact of AI for improved fraud detection? The biggest barriers are implementation challenges: scarce data science resources to develop models, long deployment timelines and difficulties bringing solutions to market, despite proven concepts. These roadblocks lead to one verdict: 48% ranked ease of deployment as the most critical success factor for AI.

Importance of components for the success of your current/future AI infrastructure



*APPF: Acquirers, payment services providers and payment facilitators.

Accelerating AI adoption

The message is clear: Financial institutions want off-the-shelf AI delivering quick time to value without major in-house investment. Models should come pretrained on vast labelled transaction data to detect known and emerging fraud patterns.

Vetting vendors is also key. Financial institutions should look for seasoned partners with specialised AI engineering expertise and financial services experience to ensure robust, nuanced models. An experienced partner can also develop global models leveraging divergent data patterns across geographies and ensure rigorous testing and validation that can prevent performance degradation over time.

Payments fraud is an arms race. Static rules grow outdated as criminal tactics rapidly evolve. AI's continuous learning is better positioned to track this dynamism. As digital transactions explode, fraud attempts will too. AI holds huge promise to counter this threat as AI adoption accelerates.

The optimal strategy is collaborating with the right vendors that provide ready-to-deploy AI tailored to fraud use cases. Specialised expertise in the field helps ensure quick implementation without overtaxing internal data science teams.

For example, Brighterion, a Mastercard company, offers pre-built AI models drawing on decades of payments industry experience. Our solutions aim to accelerate time to value and bolster fraud defence with minimal in-house lift. But the window for action is closing fast.

Tighter fraud prevention and AI go hand in hand — and both are indispensable to the future of digital banking. The payments ecosystem must collaborate to realise AI's potential. With so much at stake, the time for progress is now.

Mastercard's new global AI Centre will unlock AI's potential

Rohit Chauhan
Executive Vice President,
Artificial Intelligence

Today, we stand at the brink of significant technological advancement. With its ability to create new content and predict a whole series of next steps, generative AI is poised to transform everything from customer experiences to entire industries.

It's against this backdrop that we unveiled our latest global Centre for Advanced AI and Cyber Technology in Dubai in August. An initial focus of the Centre will be battling financial crime, securing the digital ecosystem, and driving inclusive growth in the United Arab Emirates (UAE) and beyond. In addition, we're partnering with the UAE government to increase AI capabilities and readiness across the region. Together, we'll deliver greater value for our customers and reinforce trust in the digital ecosystem.

In the spirit of driving innovation and fostering technical talent, we also announced a partnership with the Rochester Institute of Technology (RIT) in Dubai. Through guest lectures, onsite training at our Centre, and eventually an AI curriculum, we'll develop talent in the region and accelerate innovation. These efforts will empower the next generation of RIT graduates to become leaders in AI, unlocking the promise that AI holds globally.

The Middle East is a hub for innovation as it undergoes a rapid technological shift. Investments in digital transformation are expected to double over the next few years in the Middle East, and PwC estimates that AI will contribute $320 billion[8] to the region. Establishing our latest Centre and building strategic partnerships in AI will help us address some of today's most pressing challenges, including reducing fraud while helping more people access financial services.

Our efforts in Dubai – and globally – represent the latest in a series of investments we've made in Advanced AI, with existing centres in the U.S., Canada and India. To date, we have made use of AI most significantly and successfully in our efforts to enhance cybersecurity and user experiences. By applying a sophisticated AI engine, we protect more than 125 billion transactions from fraud every year – at speed and scale. Our AI-powered solution Safety Net, which protects issuers and acquirers from large-scale fraud events, prevented more than $20 billion in fraud over the past 12 months alone.

Together with our partners, we see so much promise for AI. Through continued innovation and investment, much more is possible.

IDENTITY

21 The road to data excellence >

24 Industry best practices for e-commerce fraud detection >

26 Supercharge your KYC with digital identity verification >

IDENTITY

The road to data excellence

Chris Reid
Executive Vice President,
Identity

The digital world has made it easier than ever to connect and transact online. So how do you know your customers are who they say they are? The answer is in how you leverage data to help separate the good customers from the bad.

Data is fundamental

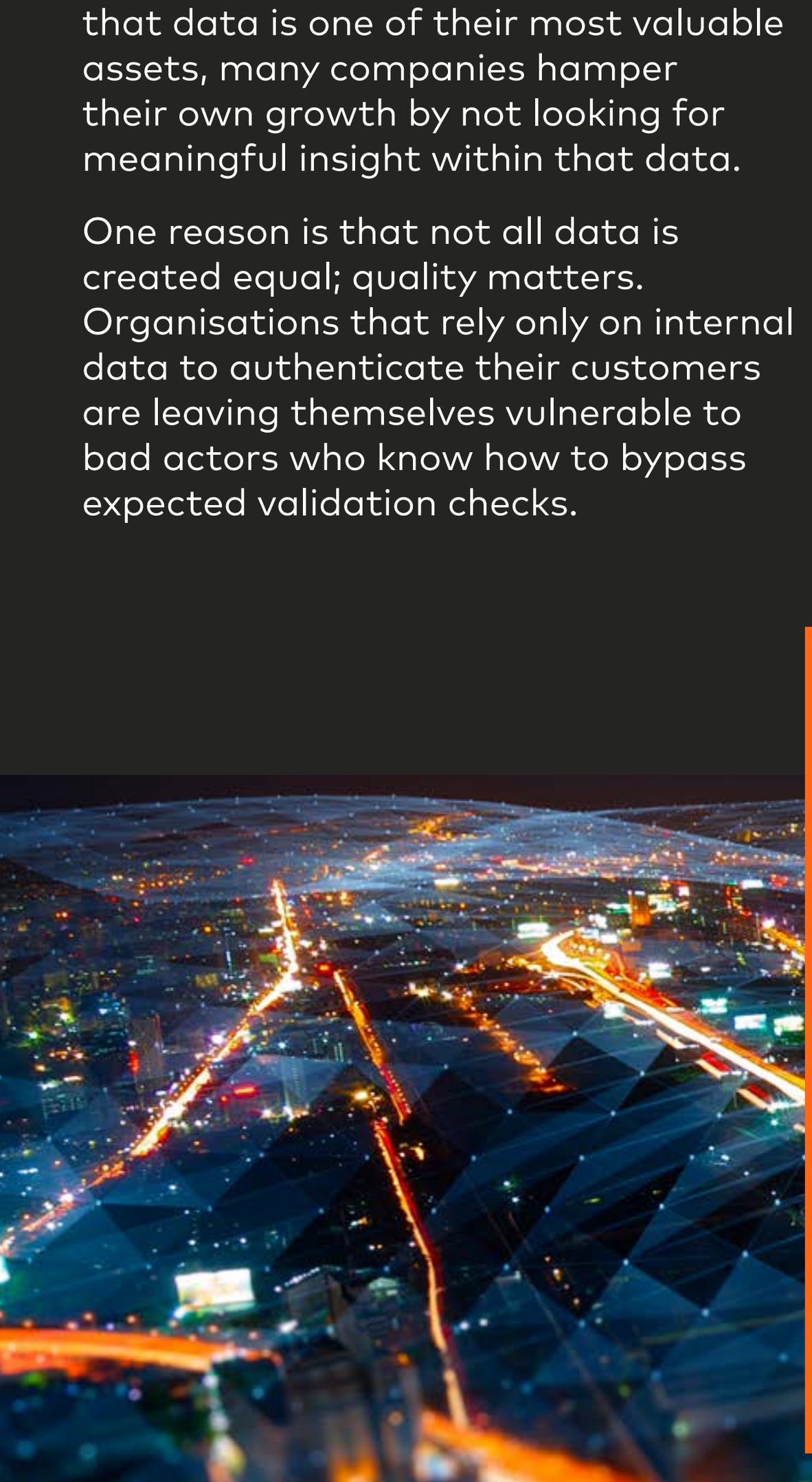
Data is the foundation of any organisation, but the key is how you use that data to improve business decision-making. While a recent Experian report shows that 85% of organisations agree that data is one of their most valuable assets, many companies hamper their own growth by not looking for meaningful insight within that data.

One reason is that not all data is created equal; quality matters. Organisations that rely only on internal data to authenticate their customers are leaving themselves vulnerable to bad actors who know how to bypass expected validation checks.

Complementary data can add context and drive differentiation

To combat the surge in synthetic identities and identity fraud, businesses need to enhance their internal data with the right complementary data.

'When it comes to deriving meaningful insights from your data, you want to invest in technology that adds context across time and geography', explains Mastercard's Vice President of Global Commercialization, Identity, Dr. Steve Marsh. 'This will enrich business logic and create stronger features to power machine learning models, all of which increases your ability to verify an identity and prevent even the most sophisticated fraud'.



At the end of the day, businesses need data that helps them answer two fundamental questions:

- Is this person real?
- Is this person who they claim to be?

Answering these questions means being able to link the digital identity to the person and then analyse how they interact and behave online.

Key criteria for data excellence

When evaluating identity verification software and data providers, it's important to ensure they meet the **following criteria**:

1

Authoritative third-party data

In the global digital economy, internal data is not enough. First-party data must be corroborated with authoritative third-party data that is approved and licensed for specific uses through trusted, quality sources.

2

Diversity

What do we mean by data diversity? That the data does not have an intrinsic bias because of how or where it was sourced. Traditional identity verification data sources tend to use a narrow set of collection methods, which can constrict the scope of identities they have access to.
A classic example is a credit bureau, which collects data only through credit applications. This creates an intrinsic bias in their dataset, because it pulls exclusively from people who need to and can apply for credit.

3

Efficacy

Good data strategies analyse the data and test it against customer use cases. Data must improve a tool's ability to identify good customers and stop bad actors; otherwise it should not be licensed. The authoritativeness of the data has to be judged by whether intrinsic bias creates inaccurate analysis. Look for identity verification data that is not scraped from the web but instead comes from sources with a vested interest in accuracy.

4

Privacy and security

Data providers should meet all the data privacy and compliance requirements of their country. For example, if they operate in the European Union they should show that they are General Data Protection Regulation compliant. They should also sign contractual agreements that they have given all necessary notices and obtained all necessary consents before an identity verification solution can use that data in their products and services worldwide. It's critical to choose a partner that's not only compliant but embraces data privacy as part of its company's DNA. Data privacy practices should be held to the highest standards.

5

Cross-border

Most organisations have only local or customer-specific networks. This limits their ability to provide the best value for the customer. Identity verification must be offered no matter where customers run their businesses.

85% of organisations agree that data is one of their most valuable assets

The Identity Engine difference

Our Identity Engine enables organisations to perform robust identity verification, combat fraud, build trust and grow revenue with a frictionless customer experience.

The Identity Engine includes two distinct and mutually exclusive data sources — Identity Graph and Identity Network — that cover all the above criteria and more.

The Identity Graph contains third-party licensed data from authoritative providers that is used to create a robust representation of a person's digital identity. It validates five key elements — name, email, phone, IP and address — and determines how they are linked to one another. The Identity Graph can answer questions like: Does this email belong to the customer? Is this physical address valid? Is the address residential?
Is this phone carrier historically risky?

The Identity Network is our proprietary first-party data asset aggregated from real-world digital interactions. Using sophisticated machine learning and data science, it predicts fraudulent behavioural patterns by analysing how any or all of the five identity elements are interacting and being used online. The Identity Network can answer questions like: When was the email first seen in a digital interaction? Has there been an increase in the number of interactions from this email/address/phone/IP in the past hour? Are there any other anomalies in the use of the identity elements?

'We use these two data assets, along with sophisticated machine learning capabilities, to power our global APIs and SaaS solution', says Marsh. 'This enables us to see not only if the data inputs go together, but if they are being used as expected. For example, the graph would recognise that a fraudster was using the same email in real time across global data centres in Singapore, North America and Germany. As a result, a higher risk score would be associated with accounts using that phone number'.

Access to both the Identity Graph and the Identity Network provides organisations with a comprehensive view of their customers' digital identities and their associated risk.

The right data can empower a business to truly know its good customers. More importantly, working with an authoritative global data provider that prioritises diversity, efficiency and privacy can make all the difference when it comes to fraud protection.

Industry best practices for e-commerce fraud detection

$48 billion

Payment fraud alone is estimated to cost online retailers some $48 billion worldwide this year

Jaime Goodman
Senior Vice President, Commercialisation Strategy, Identity

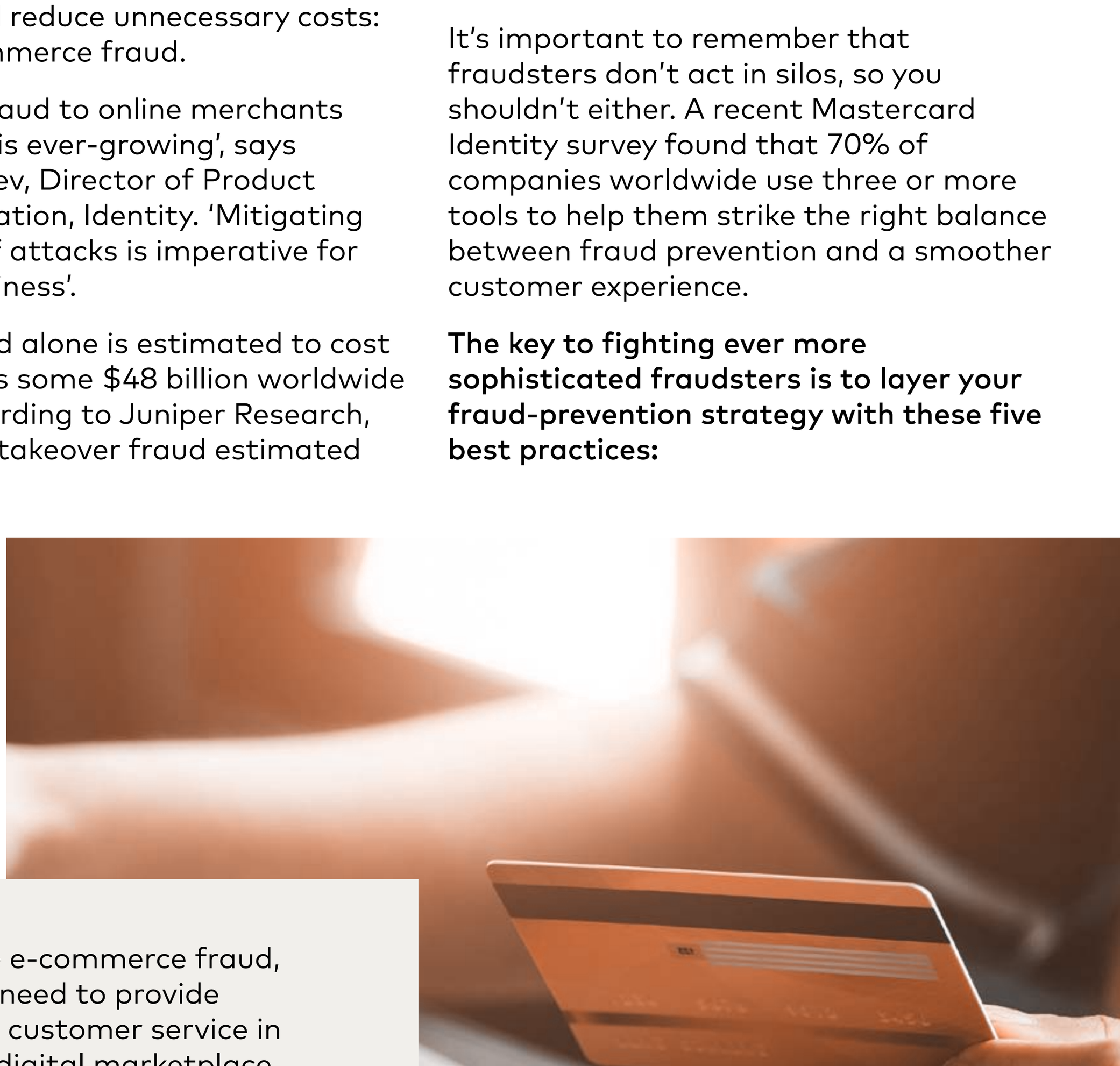
In a hypercompetitive market and a fluctuating global economy, online retailers must be strategic when it comes to attracting new customers, staying on top of profit margins and mitigating sophisticated fraud attacks. One effective way that online retailers can operate more efficiently and reduce unnecessary costs: prevent e-commerce fraud.

'The cost of fraud to online merchants big and small is ever-growing', says Milena Babayev, Director of Product Commercialisation, Identity. 'Mitigating these types of attacks is imperative for staying in business'.

Payment fraud alone is estimated to cost online retailers some $48 billion worldwide this year, according to Juniper Research, with account-takeover fraud estimated to cost merchants $343 billion over the next five years. Then there's the more insidious 'friendly fraud', or charge-back abuse, when a consumer makes an online purchase and then asks their bank to refund their money after they receive the product or service.

It's important to remember that fraudsters don't act in silos, so you shouldn't either. A recent Mastercard Identity survey found that 70% of companies worldwide use three or more tools to help them strike the right balance between fraud prevention and a smoother customer experience.

The key to fighting ever more sophisticated fraudsters is to layer your fraud-prevention strategy with these five best practices:



To mitigate e-commerce fraud, merchants need to provide exceptional customer service in a crowded digital marketplace. Partnering with a payment processor to conduct e-commerce fraud checks can help.

1

Automate decisioning with AI and machine learning

AI has emerged as a powerful tool against e-commerce fraud. Technologies such as machine-learning algorithms can analyse a significant amount of data and detect anomalies that may point to fraudulent activities. By automating decisioning with AI, merchants can make more confident risk decisions on a much faster, grander scale.

When it comes to e-commerce fraud, AI-powered fraud-management systems can detect and prevent payment fraud, identity theft and regular phishing attacks. Better still, they can adapt and, over time, learn new fraud patterns and the latest trends, further improving detection capabilities.

By integrating AI-based technology with identity-verification solutions, merchants can build their own rules. This not only provides a more comprehensive approach to e-commerce fraud prevention but also reduces the need for manual reviews, allowing for faster acceptance rates and creating better business outcomes.

2

Partner with a robust data network

Our Identity Network, for example, uses data aggregated from more than 200 million monthly anonymised, real-world queries to predict fraudulent versus legitimate interactions. It does this by analysing patterns in how identity elements are being used online. Partnering with a robust data network like Mastercard Identity empowers merchants with the information they need to make faster, more confident risk decisions.

3

Partner with a trusted payment processor

To mitigate e-commerce fraud, merchants need to provide exceptional customer service in a crowded digital marketplace. Partnering with a payment processor to conduct e-commerce fraud checks can help. Payment processors can better manage customer charge-backs (and friendly fraud attempts), as well as security compliance details and data storage.

4

Implement step-up authentication according to the risk profile

Deciding on when, how and where to introduce step-up authentication during a transaction is the ultimate decision. At Mastercard, we want to ensure that legitimate customers can transact frictionlessly. But we also enable businesses to choose 'strategic friction' when needed, so that a merchant can send a transaction for additional authentication based on the risk profile of the consumer.

Ultimately, the strategic differentiator when it comes to preventing e-commerce fraud without creating undue friction is verifying that the consumer is who they say they are. Merchants that incorporate model-derived signals — like our Identity Risk Score, Network Score and IP Risk Flag — into their own risk models can better predict a customer's risk profile and streamline their identity verification and authentication process.

'A high-risk score indicates a riskier transaction and therefore warrants a necessary layer of friction', says Babayev. 'A low-risk score? That customer can enjoy a seamless, friction-free transaction experience'.

5

Ensure your fraud prevention tools are best-in-class

Detecting and preventing e-commerce fraud while providing an excellent, seamless customer experience is an ongoing challenge for merchants around the globe. And while consumers may want it easy, they also expect security. Merchants that integrate security solutions that don't get in the way of a great customer experience will come out on top.

Supercharge your KYC with digital identity verification

Michael Pettibone
Vice President of Global Strategy, Growth and Development, Identity

New technologies, new players, new regulations and new markets are transforming the financial industry. Now more than ever, financial institutions must embrace a digital modernisation strategy or risk becoming obsolete.

A digital economy needs a digital solution

In our ever-evolving digital-first economy, where is your focus? A booming digital economy means global businesses have more new customers every day. But how do you know if your customer is who they say they are? It's not enough to look at just one or two pieces of identifying information (such as email address or phone number) and call it a day. Instead, today's businesses need a comprehensive view. To build a fraud strategy only around legacy systems and traditional Know Your Customer (KYC) and anti-money laundering (AML) processes is to open the doors to synthetic identities, promotion abuse of new digital products and account-opening fraud.

The fact is, while KYC is the first step in preventing fraud and ensuring compliance, it shouldn't be the last. Financial organisations worldwide need to layer KYC with complementary risk assessment tools for enhanced identity verification. This can create a seamless customer experience that optimises acquisition and onboarding costs, reduces operational costs and mitigates fraud loss in this new digital era.

KYC checks cost the average bank approximately **$60 million** per year

A competitive market needs a comprehensive, real-time process

As more consumers turn to online accounts, verifying digital identities is essential and needs to happen fast, because with the rise of challenger banks and other digital-only financial services it's easier than ever for customers to abandon the onboarding process and move on to a competitor. A process that validates a digital identity without adding undue friction needs to be front of mind to encourage new users to complete onboarding.

> 'To stay competitive in the digital economy, your consumer's experience from the very first connection — account opening — can make or break the lifetime relationship', says Chris Reid, executive vice president of Mastercard Identity.

The identifiers captured during traditional KYC — such as physical address, national ID number and birthdate — are not only static but also tangential to a digital identity. That's why it's critical to layer capabilities that enhance verification. Our Account Opening API, for example, makes it easy to evaluate the risk of dynamic digital identity elements like email, name, address, phone and IP address. This technology also looks at how these elements are linked and, in turn, scores risk behaviour in real time. Institutions can then adjust and streamline onboarding for each applicant based on their individual risk score. For example, a high-risk score might warrant additional onboarding steps like requesting additional documents, while applicants who score as low-risk can enjoy a more streamlined experience.

Cost and revenue optimisation

Of course, enhancing your KYC and identity verification process at onboarding doesn't just benefit your consumers. It can benefit your bottom line, too. Let's face it: The costs for companies of new customer onboarding are significant. And running each new applicant through your traditional risk assessments, such as KYC, AML, credit checks and so forth, is more costly still. Trust us, we've run the numbers.

> 'According to Consult Hyperion, the latest estimated cost of a KYC compliance check ranges from $13 to a whopping $130', injects Reid. 'That adds up to approximately $60 million per year for an average bank'.

In fact, a recent global study conducted by Fenergo suggests that financial institutions spend millions of dollars every year inefficiently onboarding clients.[9] More than half say they're completing up to 60% of their KYC review tasks manually, with 50% of that cohort also spending up to $3,000 to complete just one KYC review. Therefore, it comes as no surprise that running a low-risk customer through unnecessary step-up verification costs you not only in potential customer drop-off but also in expensive, time-consuming processes.

'An advanced, real-time digital identity verification tool can save businesses money, free staff up for more meaningful work and ensure a smooth experience for legitimate customers', says Reid. 'Identity fraud is a complex and constantly evolving problem, but these cutting-edge solutions can keep it from harming your bottom line'.

Fighting fraud

Embracing a layered approach to identity verification not only optimises the cost of onboarding but also mitigates fraud. Synthetic identity fraud is the fastest-growing fraud, according to the US Federal Reserve. Letting these synthetic identities, or a combination of fabricated credentials, slip through the cracks of static legacy processes costs financial institutions upwards of $6 billion a year. When you add this to the cost of skewed customer acquisition costs associated with promo abuse run rife, you fast realise that leveraging fraud-fighting technology within a multilayered platform is the only way to go.

CYBER

29 Mastercard brings its latest AI capabilities to the fight against payment scams >

32 Keep it simple: The impact of DORA and NIS2 on third-party risk management >

35 What lies ahead: The future of digital banking >

38 How to identify and manage VASP counterparty risk >

41 The future of cyber risk management >

Mastercard brings its latest AI capabilities to the fight against payment scams

207,372 APP scams were reported in the UK in 2022, amounting to gross losses of **£485 million**

We recently sat down with Johan Gerber at Mastercard to learn more about how technology can stop fraudsters in their tracks.

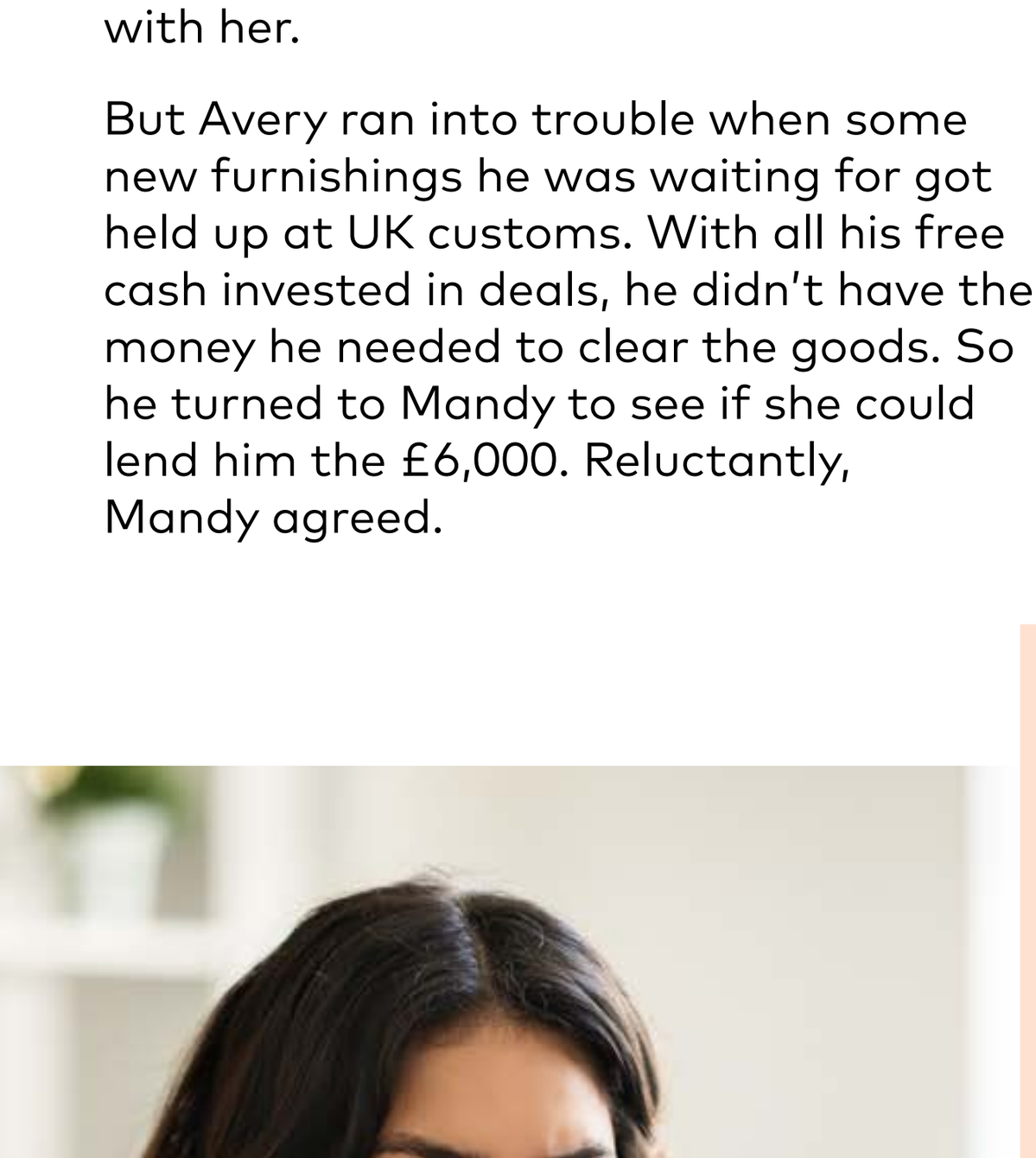
Johan Gerber
Executive Vice President,
Security and Cyber Innovation

When Mandy met Avery (not their real names), she thought she had found someone with whom she could forge a real relationship. Avery was a divorced father and a boxing promoter. His life appeared to be incredibly exciting and, best of all, he seemed completely smitten with her.

But Avery ran into trouble when some new furnishings he was waiting for got held up at UK customs. With all his free cash invested in deals, he didn't have the money he needed to clear the goods. So he turned to Mandy to see if she could lend him the £6,000. Reluctantly, Mandy agreed.

And then she agreed again. And then she agreed again. By the end of their relationship six months later, she had lent Avery £60,000. But of course, he would never pay it back, because Avery wasn't a loving boyfriend. Avery was a romance fraudster.[10]

Mandy is not alone. As security for banking and payments has become increasingly advanced, fraudsters have shifted their focus to impersonation tactics. Masquerading as family members, online stores, debt collectors or romantic partners, they convince victims to send them money, thinking the transfer is to a legitimate person or entity.



Stopping these authorised push payment (APP) scams, in which the payment was authorised but fraudulently induced, is enormously complicated. In 2022, 207,372 APP scams were reported in the UK, with gross losses of £485 million (US$618 million)[11]; **they now account for 40% of UK bank fraud losses**. Experts predict these crimes could cost $4.6 billion in the US and the UK alone by 2026.[12]

However, the tide is turning. Mastercard is joining forces with UK banks to take the fight to the fraudsters with its one-of-a-kind, AI-powered Consumer Fraud Risk solution, now live in the UK.

How do these scams work?

They take two primary forms. One is based on sophisticated social engineering and manipulation — tricking people into transferring funds and making them think they are doing it for a legitimate cause. For instance, the fraudster can spend months fabricating an online romance with you and convince you to lend them money. Or they use online marketplaces to advertise deals too good to be true. Some even exploit victims' illnesses or disabilities, conning sufferers or family members into paying for expensive medical equipment that never arrives.

The second type of scam is designed to trick a consumer into handing over their banking account access credentials, allowing criminals to take control of the account. For example, maybe a scammer digs up some information about you and then uses it to convince you they're from your bank. 'Your account has been taken over! We need to move your money fast!' You send them your login credentials or the one-time password, and the balance goes straight into their pocket.

These scams all have elements in common: urgency and the demand for an advance payment or a temporary loan.

Who is most at risk?

Everyone, everywhere. APP scams are quickly becoming the go-to for fraudsters around the world, including in the US and Canada. The collective loss is running into the billions, even though these scams represent less than 0.01% of transactions. Elderly and retired people are frequent victims, and the deceit often wipes out their retirement savings. Every scam is personal to the consumer.

Why can't banks just block the transactions?

Spotting APP fraud among the millions of payments made every day is incredibly challenging. These transfers are authorised by the consumer, meaning they pass all authentication checks. The consumer is 100% convinced that they are doing the right thing. It's not like credit card fraud, where the cardholder doesn't necessarily even know about the transaction until the issuer bank declines it.

Once the money is sent, it can move through multiple banks in a matter of hours. Banks lose sight of funds once they are transferred to another bank, so subsequent transfers have been impossible for the initial institution to trace. That's why AI prevention and monitoring tools are crucial in the fight against APP fraud.

What's Mastercard's solution?

We know that organised criminals disguise scammed funds by moving them through a series of mule accounts. So for the past five years we've worked with UK banks to follow the flow of funds through these accounts and close them down. Building on our unique view of account-to-account payments, we developed an AI tool called Mule Insights Tactical Solution that tracks the disbursement of illicit funds.

Now we've overlaid that network-level data with other relevant factors — such as account names, transaction history and the payee's links to accounts associated with scams — to create an AI solution called Consumer Fraud Risk (CFR). Using our AI capabilities, CFR evaluates how a recipient account operates and traces its relationships to other transactors. From that it infers the risk of an impending payment and delivers a fraud score in real time, so our partner banks can intervene to stop scam transfers before funds leave a victim's account.

How does it work?

Because fraud is such a complex problem, our solution takes a multilayered approach. First, because scammers need to move stolen funds through mule accounts to make it untraceable, CFR prevents them from taking over existing accounts or using synthetic or stolen identities to open new accounts. Also, through its analysis, CFR has derived the most telling traits of a mule account, allowing the software to identify suspicious accounts even before they are used.

On the other side of the equation, by analysing victims' accounts, CFR can infer the primary characteristics of an account likely to be targeted. Then, understanding the anatomy of a scam allows us to identify distinctive patterns at the transaction level.

Putting all this together through the power of scalable AI — and combining it with the bank's understanding of what is normal for both the sending and receiving accounts — makes it possible to derive an accurate risk assessment.

What are the results so far?

TSB was one of the first banks to adopt CFR, and they are already using it to great effect. In just four months, CFR has dramatically improved TSB's fraud detection. If CFR performs equally well at all UK banks, **we can expect to prevent close to £100 million a year[13] in scam payments across the UK.**

When used in conjunction with other insights about customer behaviour, CFR has helped banks create targeted strategies to identify and stop several types of APP scams — in particular purchase scams, impersonation scams and romance scams. Purchase scams now account for 57% of scams in the UK and remain a notorious pain point for banks.[14]

But in addition to technical solutions like ours, government policy and public education are key to ensuring that people are aware of this kind of scam and how to avoid falling victim to it.

Where is CFR available?

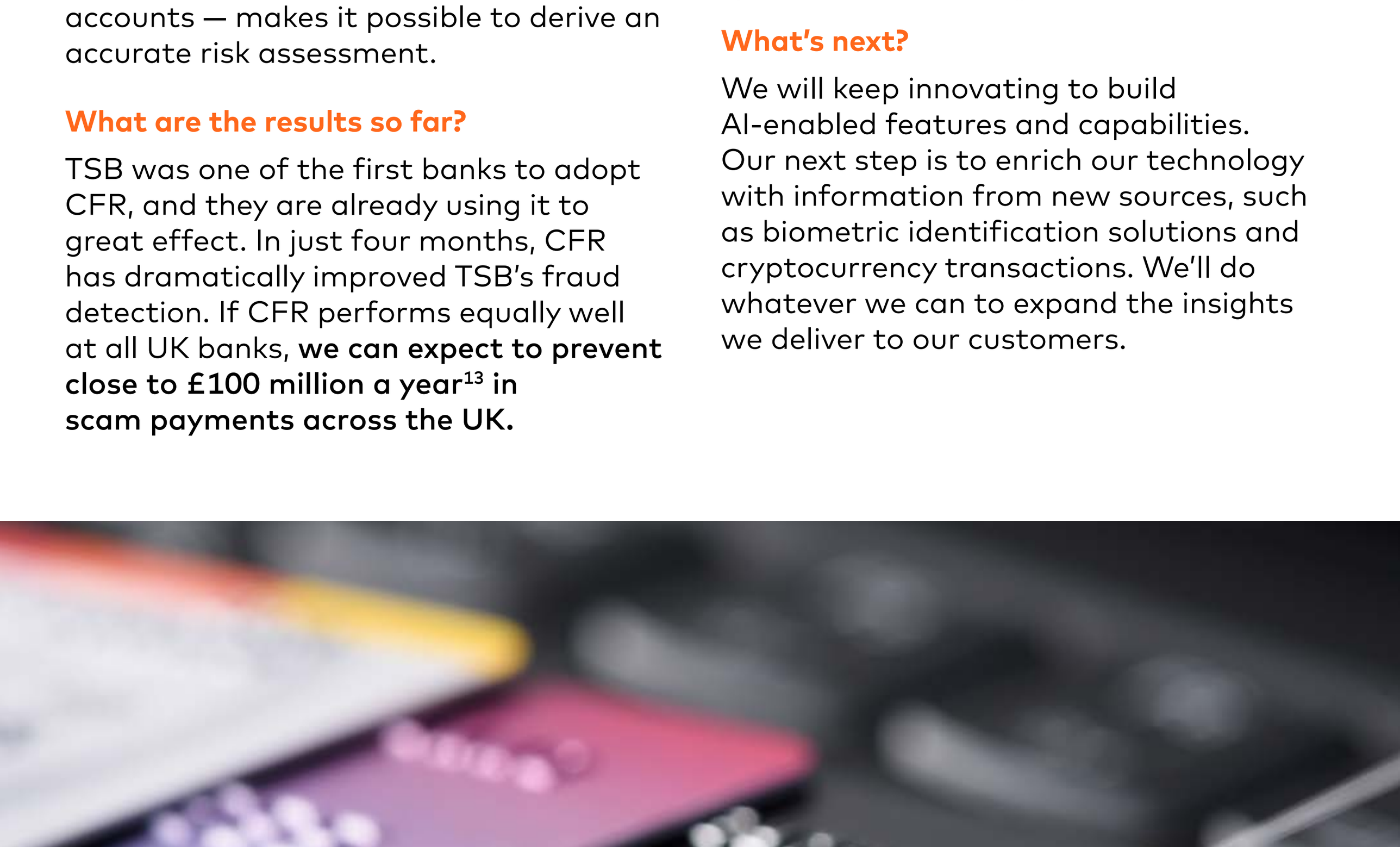
At the moment, we're partnering with nine UK banks, including Lloyds Bank, Barclays, Monzo, NatWest and TSB, with more expected this year.

Are you planning to roll this out beyond the UK?

Yes, we are looking at other markets with mature real-time payment systems and challenges with APP fraud.

What's next?

We will keep innovating to build AI-enabled features and capabilities. Our next step is to enrich our technology with information from new sources, such as biometric identification solutions and cryptocurrency transactions. We'll do whatever we can to expand the insights we deliver to our customers.



CYBER

Keep it simple: The impact of DORA and NIS2 on third-party risk management

Rigo Van der Broeck
Executive Vice President, Cyber and Intelligence Solutions

In a recent webcast, Roger Ison-Haug, the chief information security officer at the weather forecasting firm StormGeo and a prominent authority on cybersecurity trends in Europe, shared insights as a key customer of RiskRecon from Norway. The discussion focused on the strategies and approaches that organisations should adopt to adhere to DORA and NIS2 regulations concerning third-party risk management.

An important recurring theme throughout the session was his emphasis on simplicity.

> 'Despite the risk of this digital world, we are not powerless', Ison-Haug said. 'If we have structure, methods and practices that are tested, we can significantly reduce risk and increase our control of the digital security'.

What are the DORA and NIS2 regulations?

The Digital Operational Resilience Act, or DORA, is a European Union regulation that creates a binding, comprehensive information and communication technology (ICT) risk management framework for the EU financial sector. DORA establishes technical standards that financial entities and their critical third-party technology service providers must implement in their ICT systems by January 17, 2025.

In January 2023, the EU adopted a new version of the Network and Information Security Directive. Dubbed the NIS2, it aims to get the EU up to speed and establish a higher level of cybersecurity and resilience within its member organisations.

What steps can you take to meet these standards within your TPRM programme?

Keeping it simple when meeting DORA and NIS2 standards is essential for organisations striving to maintain a robust and efficient data management framework. DORA compliance ensures that businesses adhere to data protection and privacy regulations, safeguarding sensitive information and earning the trust of customers, partners and regulatory bodies. Emphasising simplicity in compliance efforts brings numerous benefits, ranging from reduced operational complexity to enhanced risk management and improved customer satisfaction.

Here are nine reasons why simplicity is vital in achieving and maintaining DORA compliance:

1

Clarity and understanding

Simplicity in DORA and NIS2 compliance promotes clarity and understanding throughout the organisation. Complex and convoluted processes may lead to confusion among employees, making it difficult for them to follow guidelines and procedures accurately. Simplified compliance guidelines, on the other hand, ensure that everyone involved comprehends their roles and responsibilities, facilitating smooth implementation of compliance measures.

2

Ease of implementation

A straightforward compliance framework allows for easier implementation across different departments and business units. When policies and procedures are simple, employees can quickly adopt them without significant disruptions to their daily tasks. This streamlined approach reduces resistance to change, promoting a culture of compliance within the organisation.

3

Cost-effectiveness

Simplicity in DORA and NIS2 compliance also translates into cost-effectiveness. Complex compliance measures often require substantial investments in specialised tools, training and personnel. By simplifying the process, organisations can optimise their resource allocation and avoid unnecessary expenses while still maintaining the required level of data protection.

4

Faster response to changes

The regulatory landscape is constantly evolving, and compliance requirements may change over time. A simple DORA and NIS2 compliance structure allows organisations to be more agile in adapting to these changes. Flexibility in compliance measures ensures that businesses can respond quickly to new regulations or amendments, reducing the risk of noncompliance and potential penalties.

5

Reduced human error

Complex compliance processes are prone to human error, which can lead to data breaches and compliance violations. Making processes simple minimises the chance of mistakes and ensures that critical compliance tasks are consistently carried out correctly. This reduces the likelihood of data leaks and noncompliance incidents.

6

Enhanced risk management

DORA and NIS2 compliance aims to mitigate risks associated with data management and privacy. A simplified approach allows organisations to identify and address potential risks more effectively. By streamlining processes, businesses can better focus on critical risk areas and implement appropriate safeguards to protect sensitive data.

7

Improved customer trust

Customer trust is paramount in any business, and compliance plays a significant role in building and maintaining that trust. A simple and transparent compliance framework assures customers that their data is being handled responsibly, fostering a positive perception of the organisation's commitment to data protection.

8

Scalability and expansion

As businesses grow and expand, compliance requirements may become more complex. However, a simple DORA and NIS2 compliance foundation provides a solid basis for scalability. It enables organisations to expand their operations while easily integrating new compliance measures without overburdening their resources.

9

Standardisation and consistency

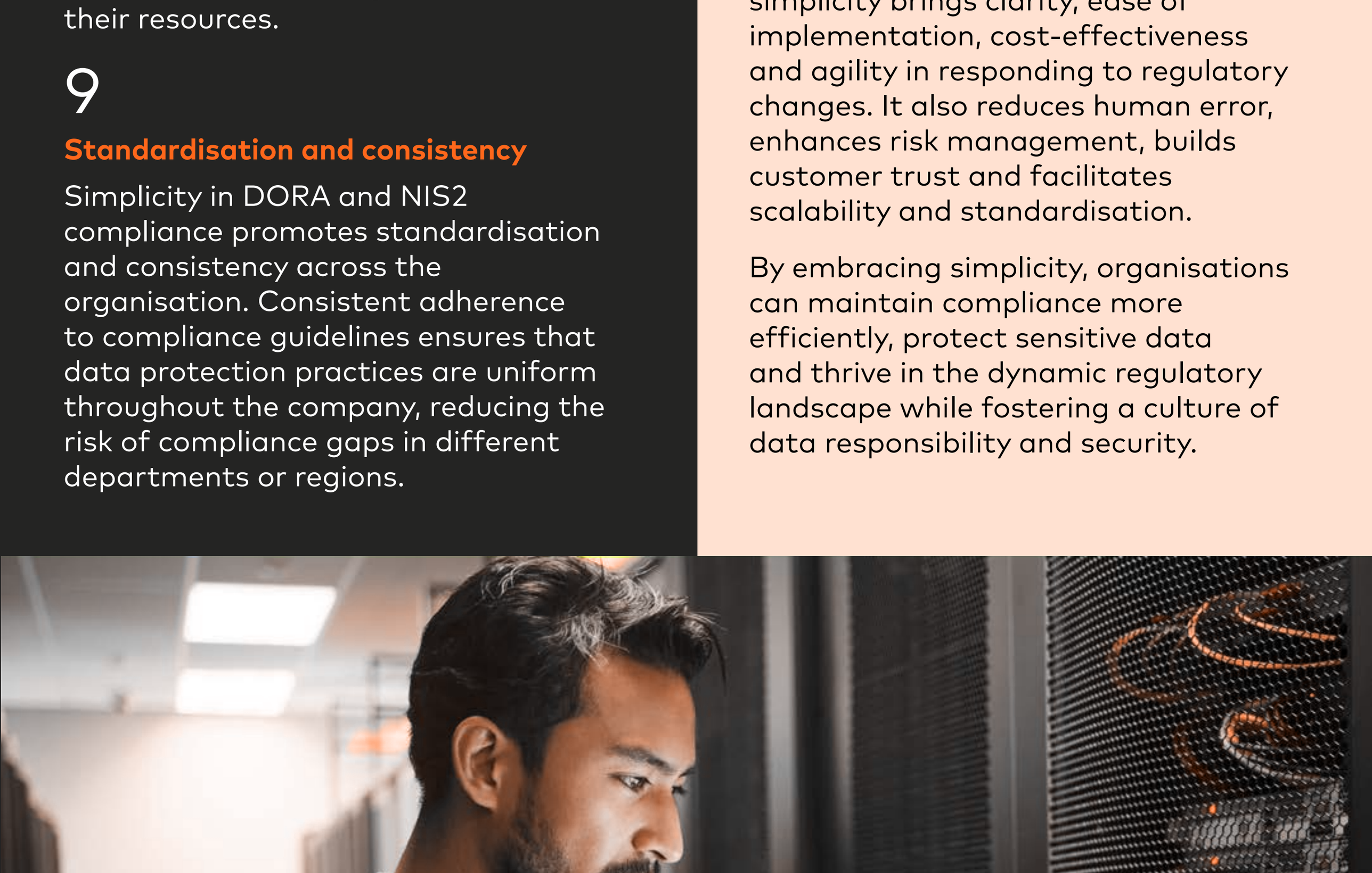
Simplicity in DORA and NIS2 compliance promotes standardisation and consistency across the organisation. Consistent adherence to compliance guidelines ensures that data protection practices are uniform throughout the company, reducing the risk of compliance gaps in different departments or regions.

The importance of monitoring risks from third-party vendors

Looking at DORA and NIS2 through a third-party risk management lens, it's important that your organisation has total visibility into risks coming from all the vendors in your portfolio. As Ison-Haug keenly put it during the webcast, 'We need to ensure that the third parties [in our vendor network] have appropriate security measures to protect our data. Periodic risk assessments, periodic audits and continuous monitoring are some of the key elements that you need to adhere to if you want to even be close to meeting the standards'.

When it comes to meeting DORA and NIS2 compliance requirements, simplicity brings clarity, ease of implementation, cost-effectiveness and agility in responding to regulatory changes. It also reduces human error, enhances risk management, builds customer trust and facilitates scalability and standardisation.

By embracing simplicity, organisations can maintain compliance more efficiently, protect sensitive data and thrive in the dynamic regulatory landscape while fostering a culture of data responsibility and security.



What lies ahead: The future of digital banking

If issuers and merchants can build trust, cardholders will follow

50% of cardholders log into their digital banking channels at least once a week from a personal device

Gaurav Mittal
Executive Vice President, Ethoca

The past five years in banking have seen a sea change as fintechs have disrupted every sector. If this revolution has proven one thing beyond a doubt, it's that digital experiences are paramount, and issuers and merchants that don't meet consumers' evolving needs are destined to fall behind.

Many activities that were historically the responsibility of financial institutions have shifted to fintechs as consumers have sought better and easier experiences.

The success of third-party applications in sending money abroad and of third-party wallets in making payment transactions are just two areas where an inability to keep up with changing expectations has resulted in a loss of market share for issuers. Similar examples abound for merchants.

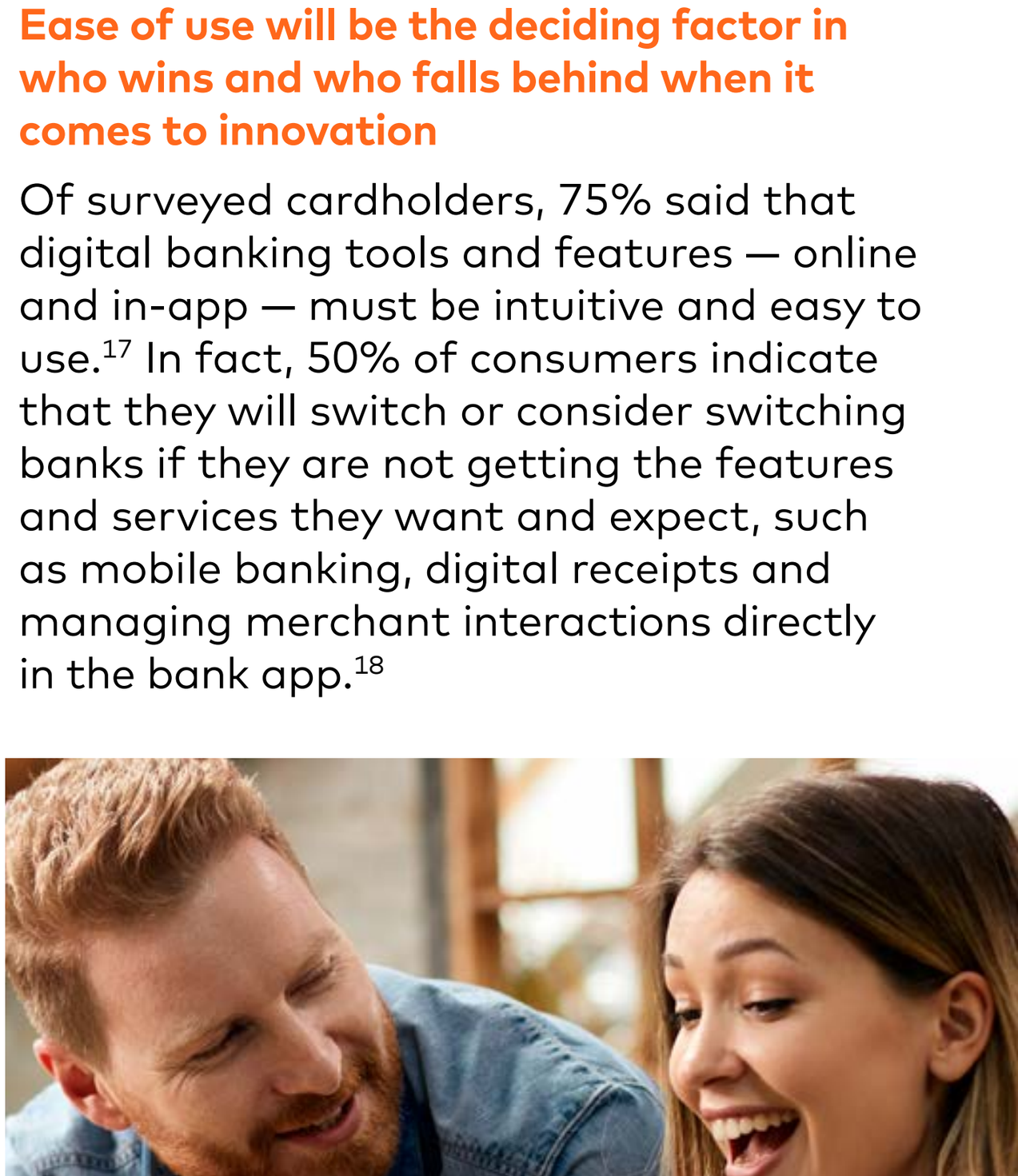
This shift serves as a valuable lesson for incumbents as they look to the future. Research shows that ease of use remains key for consumers, who also want more visibility into, and better control of, their financial lives.

Digital bank channels remain one of the most used — and trusted — channels by which consumers can manage their finances

Fifty percent of cardholders log into their digital banking channels at least once a week from a personal device, and of those, more than 64% are using smartphones to access their accounts.[15] What's more, over 70% of consumers believe banks and financial institutions provide a more secure online experience. While individual experiences on merchant websites or apps will still exist, brands that can extend their presence across payment channels and connect to their customers anywhere will be more likely to prosper.[16]

Ease of use will be the deciding factor in who wins and who falls behind when it comes to innovation

Of surveyed cardholders, 75% said that digital banking tools and features — online and in-app — must be intuitive and easy to use.[17] In fact, 50% of consumers indicate that they will switch or consider switching banks if they are not getting the features and services they want and expect, such as mobile banking, digital receipts and managing merchant interactions directly in the bank app.[18]



There is a strong desire among consumers for new features that make it easier to manage their finances with their financial institutions and the brands they support

Features that empower consumers to manage their finances and find ways to save typically rank higher on the list. Based on a recent survey Mastercard conducted with Aite-Novarica Group, digital receipts and subscription management features lead the charge: 88% of consumers want access to digital receipts for their transactions, and 85% of consumers want to manage their subscriptions through their digital banking platforms.[19] Coupons and loyalty rewards follow closely behind on consumers' list of needs and expectations.

The power of digital receipts

Among the emerging digital banking features, digital receipts have a direct benefit for everyone:

- For issuers, they create a more engaging experience, which can result in significant drops in call-centre volume
- For merchants, they provide positive brand association and help reduce potential disputes related to purchase confusion or 'first-party fraud'
- For cardholders, digital receipts give them the information they need, when and where they want it, to resolve any confusing or disappointing experience almost instantaneously, boosting brand loyalty

Subscription management can be a secret weapon

A typical consumer may have up to a few dozen subscriptions that are billed at different dates and frequencies. Tracking all these subscriptions is challenging and can make consumers feel that their financial lives are out of control, leading to merchant disputes.

Everyone wins when consumers have a view into all their subscriptions in digital bank channels, as well as the ability to cancel, pause or modify them:

- Issuers can provide peace of mind, a sense of trust and a differentiated experience
- Merchants end up with fewer disputes because they can handle cancellations directly. Some merchants have even reported that giving consumers this control results in higher, not lower, subscription rates
- Cardholders get a new level of insight, clarity and control over their subscription-related expenses

The experience-driven future of digital banking requires the right partner

The optimal path forward is one that recognises that fine-tuning the digital experience for customers can drive engagement and encourage increased spending, while also minimising fraud and charge-backs and their associated costs. Focusing on the digital experience and fraud as individual priorities may yield gains, but improving both holistically will yield even better results.

For issuers and merchants, improving their digital experience can be a costly and complicated process, as the amount of data needed is formidable. Imagine each issuer building direct connectivity to pull digital receipts from each merchant, or integrating with them for subscription controls — the complexity, time and effort would be prohibitive. Working with a partner can reduce the cost and the time to implementation.

88% of consumers want access to digital receipts for their transactions

Keeping pace with the steady drumbeat of innovation will create a future where customers are more engaged with their financial institutions and their favourite brands. It will also build trust by providing them with more actionable and transparent insights into their finances. No matter how technology or habits change over time, one thing always remains true: Meeting and exceeding customer expectations will provide businesses with long-term value and loyalty.

How to identify and manage VASP counterparty risk

Jonathan Anastasia
Executive Vice President, Crypto and Security Innovation

Despite the recent crypto winter, the virtual assets market, which includes cryptocurrencies and NFTs, has continued to grow, with total market capitalisation rising 6% over the past year to $1.09 trillion today.[20] As bank customers demand convenient pathways for buying and exchanging cryptocurrency, the virtual asset ecosystem is intersecting more often with traditional financial institutions.

This situation can be beneficial to both — banks can enable their customers to take advantage of a cutting-edge payment technology, while crypto businesses bring in new investments. However, it has also raised regulatory concerns regarding financial crime and consumer protection. What does this mean for banks?

In the past year, the market capitalisation of the virtual assets market has risen by 6% to **$1.09 trillion**

The crypto challenge

To meet consumers' demand to exchange fiat and crypto safely, it's crucial for banks to comply with regulations relating to money laundering and fraud. If they fail to do so, consumers could lose money to crypto-based fraud and scams, issuing banks could face sanctions or heightened supervisory scrutiny, and acquiring banks could expose their partners to the same dangers.

So how can banks identify suspicious activity? Although on-chain interactions are not usually visible to non-crypto businesses and entities, banks can learn a lot by evaluating each customer's choice of virtual asset service provider (VASP). As the businesses that facilitate crypto transactions, VASPs — which include exchanges, crypto ATM operators, OTC desks and wallet custodians — act as the node between the consumer and the virtual asset world. As such, they are the first and often the strongest line of defence against crime in the crypto sphere.

Many VASPs take robust measures to prevent illegal activity. But some don't. For that reason, banks should perform enhanced due diligence into the VASPs they onboard. When conducted manually, this process can be prohibitively labour-intensive, so many banks avoid VASP relationships entirely and decline all crypto transactions — at the cost of alienating customers and leaving revenue on the table.

Risk factors

It is possible for banks to make informed decisions about the risks surrounding potential VASP counterparties — given the right data and insights. These are some of the key factors that indicate whether a VASP may be involved in illegal activity:

Know Your Customer (KYC) policies

A VASP that verifies user identities is less likely to onboard applicants engaged in criminal activity. Strong KYC controls require ID verification, proof of address and other identifying information before a customer can use the service. Automated KYC verification tools can complement these processes.

On the other hand, a VASP with lax protocols may conduct limited ID verification; it might also allow deposits or withdrawals up to a specified amount with little or no KYC. The riskiest VASPs allow daily deposits or withdrawals with no information beyond an email address or phone number, which is increasingly an area of focus for regulators.

Connection to dubious on-chain entities

An analysis of transactions can reveal the extent to which a VASP has done business with high-risk or even sanctioned organisations. Exposure to criminal enterprises, darknet markets, ransomware, malware, high-yield investment programs (Ponzi schemes), online gambling, mixers or tumblers is also linked to increased likelihood of illegal activity.

Privacy coin support

VASPs that support anonymity-enhanced privacy coins (such as Monero and Zcash) are higher-risk, as these coins make it easier for criminals to hide their IDs, balances and transaction details.

Domiciled location and alignment with Financial Action Task Force (FATF)

The jurisdiction in which a VASP is licensed or conducts business is an important indicator of AML and sanctions risk. VASPs in countries that are members of the FATF or FATF-style regional bodies[21] are less likely to facilitate financial crime.

Age

The longer a VASP has been in operation, the lower its associated risk.

Fiat capabilities

VASPs that support fiat[22]/crypto trading pairs — allowing users to deposit fiat directly into (or withdraw it directly from) the exchange to fund an account — may offer criminals the opportunity to exchange cash for crypto and vice versa.

Banking relationships

If a VASP maintains a relationship with a bank known to exercise strong onboarding protocols, the institution must view the VASP as safe enough to manage with compliance controls.

Turning challenges into opportunities

Taken together, these factors can assemble an accurate picture of a VASP's level of security. However, because conditions in the cryptosphere are fluid, a VASP's profile can change — for better or worse. With thousands of VASPs around the world, it's nearly impossible for bank staff to keep up manually.

That's where AI comes in. Blockchain analytics tools can harness this sort of knowledge to strengthen risk management for banks that support crypto. The sophisticated algorithms in these software systems create highly accurate risk models to help banks identify VASPs prone to hosting criminal activity.

Armada, a blockchain analytics platform from Ciphertrace, a Mastercard company, fuses this key security information with advanced AI to broaden visibility into cryptocurrency blind spots. Analysing on-chain, off-chain and proprietary data, Armada generates a VASP risk scorecard. Based on the first five of the factors listed above, Armada's AML Risk Score represents a VASP's vulnerability to money laundering on a scale from 1 to 10. The higher the score, the higher the potential for money-laundering activity. This scorecard also provides banks with insight into card approval and denial history, cybersecurity risk, licensing status and custody data.

Another Ciphertrace service, Virtual Entity Risk Assessment (VERA), quantifies VASP risk holistically. Combining Armada's datasets with open-source intelligence and in-house expertise, VERA expands the Armada scorecard to include ratings for regulatory and reputational hazards.

As crypto — and the regulations that surround it — evolve, banks will need advanced, high-quality analytics tools to identify and mitigate risks unique to crypto and blockchain. Effective blockchain analytics tools offer a powerful buttress to virtual asset security, helping banks create a safe and lawful crypto environment. With a data-driven understanding of a VASP's risk profile, banks can make informed decisions and demonstrate sound risk management analysis to regulators.

The future of cyber risk management

Kelly White
Senior Vice President,
CEO, RiskRecon

Modern society is fuelled, funded and facilitated by digital connectivity, and it's hard to overstate the advantages and benefits of our internet-enabled systems. But at the same time, increased tech dependency means increased vulnerability.[23]

Because computer systems now underpin nearly every facet of the global economy, any threat to digital infrastructure is a threat to the entire system. It can feel overwhelming to face more existential risks than ever. But inaction isn't an option. Teams that put in the work to effectively manage their cyber risks will be equipped to safely circumvent growing cyberthreats and to capitalise on the risks worth taking.

The growing 'risk' of doing business

If you work in software engineering, IT or information security (InfoSec), at some point in your career you've probably voiced warnings that went unacknowledged. The challenge of raising widespread awareness and obtaining executive support has persevered since the earliest days of the internet.

Organisational staff members often see a disconnect between their work and risks around digital hygiene and system infrastructure. Employees might think, 'It won't ever happen to me', or, 'What I do doesn't have that big an impact on outcomes'.

Management team members, for their part, can struggle to see infrastructure and operations investments as anything other than an expense. Without a clear understanding of what a data breach or loss of operations might cost, they just don't see the need.

These communication gaps are problematic, especially as the scope and stakes of cyber risks have escalated dramatically in recent years. In the past, infrastructure and operations teams had no choice but to do their best to prevent losses with limited resources and assistance. It was incredibly difficult. Now the emergence of new threats has made it virtually impossible to stave off losses without adaptation.

Risk factors to have on your radar

In today's fast-paced, digital-first world, keeping up with the rapid changes in risk management is no small chore. Even canny business professionals may find themselves caught unawares by new developments.

Major risk factors you must have on your radar include:

Operational risk:

These days, operations can be disrupted by something as simple as interrupted internet access. If your website goes down even briefly, customers and clients can't access accounts, make purchases or contact support. If internal teams can't access critical applications or systems, even the most basic daily processes can grind to a halt. Today, systems and operations are intertwined. Server outages are just as disruptive as supply shortages, and website glitches are as frustrating as equipment failures. When businesses rely on digital systems to operate, system disruption is operations disruption.

Financial risk:

With financial systems almost entirely digital, and consumer and commercial transactions depending on stable, secure digital technology, even minor technical glitches can dramatically impact operations. What's more, the concentration of liquid assets in digital systems makes them a major target for cybercriminals.

Geopolitical risk:

Threats can be politically motivated, and organisations can be targeted based on the value they provide to their nation's infrastructure. Even private entities can be targets, since they often support economies and local communities.

ESG risk:

ESG (environmental, social and corporate governance) measures how safe a business is to invest in, partner with or otherwise support, and it comes with its own unique set of risks.

- **Environmental**

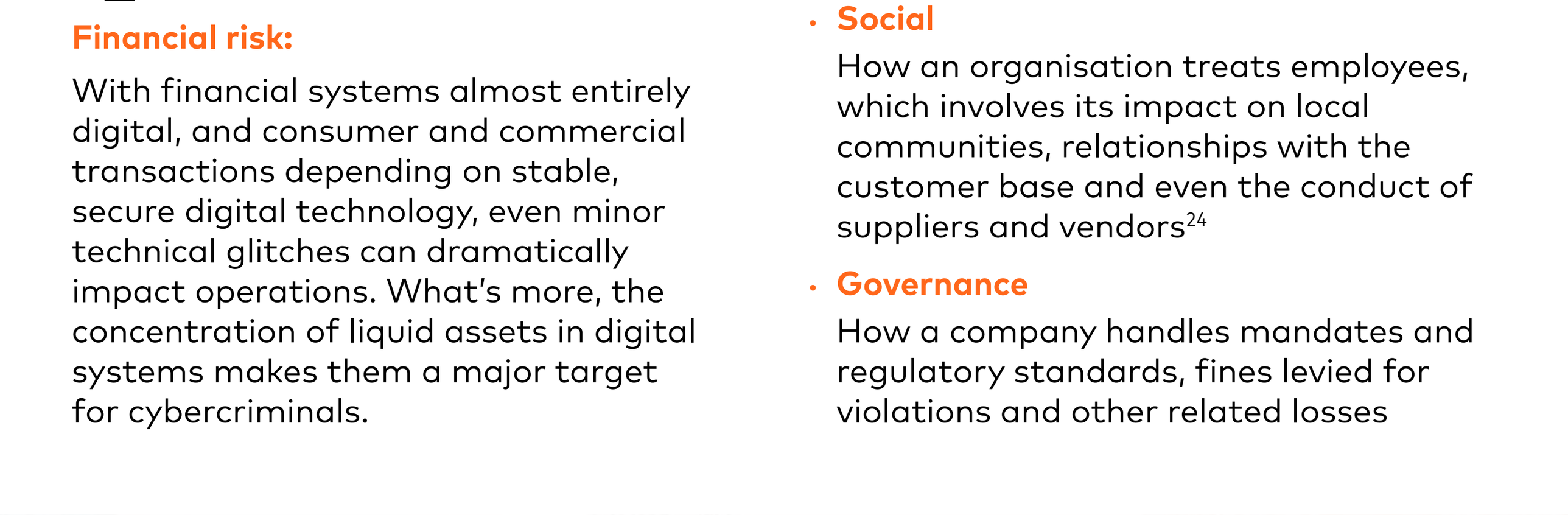
  How a company consumes natural resources, its climate impact (carbon footprint) and its treatment of animals

- **Social**

  How an organisation treats employees, which involves its impact on local communities, relationships with the customer base and even the conduct of suppliers and vendors[24]

- **Governance**

  How a company handles mandates and regulatory standards, fines levied for violations and other related losses



Modern solutions to modern problems

Keeping pace with — let alone staying ahead of — digital threats is far from easy.[25] The good news is, these are challenges every organisation faces, and entire industries are working to find effective ways to solve them. For example, there's an entire market dedicated to IT management software. These tools add convenience but also complexity. Combine them with an already unwieldy tech stack and upkeep quickly becomes untenable — both in labour and in subscription fees.

In this environment, improving security means reducing burdens and adding simplicity.[26] With IT and InfoSec teams in every industry feeling this pressure, it's not surprising to see new categories emerge almost overnight (e.g., 'digital platform conductor' tools recently developed by Gartner).

The bottom line is that, yes, vetting new software tools can be agonising. But long-promised single-pane-of-glass solutions are finally within reach.

Evolving risk management tactics

Risk management has had to alter course to compensate for major shifts in the business landscape. We've seen the emergence of new specialised fields like enterprise risk management (ERM)[27], which is built on effective methods for applying quantitative measurements to a variety of qualitative potentialities. Technology fuels many of these developments, with risk assessment solutions[28], prescriptive analytics and other data-backed tools helping teams make smarter decisions.

Successful modern risk management requires constant reevaluation and recalibration to stay in lockstep with the rapid pace of change.

The transition to frameworks

It's also critical to keep frameworks top of mind. Frameworks are to risk management and InfoSec what safety standards or SOPs are to other industries.[29] And while frameworks have been available in one capacity or another for some time, they're now at the forefront of discussions regarding cyber risk management.

Examples of cybersecurity frameworks include the National Institute of Standards and Technology (NIST) and the National Information Systems (NIS) Directive, both of which will soon be getting overhauls. Many organisations are also adopting these types of frameworks voluntarily, even as the number of industries with mandated compliance increases.[30]

Making the most of the future

In our fast-paced digital world, the risks and potential losses are staggering when compared with those of decades past. But so are the opportunities. Every business and organisation faces similar threats; it's how they manage those risks that will make a significant difference in outcomes.

Better management of cyber risk means better protection and better longevity. Attacks, breaches and other disasters are nearly unavoidable, but they're not insurmountable. Businesses that are properly prepared will be positioned to survive and thrive despite losses.

These are concerns for consumers, clients, partners and the market at large — not just businesses themselves — and brands that can prove themselves capable of navigating the hazards will earn the trust and loyalty of all stakeholders.[31]

RISK & RESILIENCY

45 Building resilience in payments >

47 How telecom providers stay ahead of third-party risk >

51 Companies can no longer ignore ESG risks >

Building resilience in payments

Laura Quevedo
Executive Vice President,
Payment Resiliency
& Platform Advancement

Recently, a bank suffered multiple outages that impacted **14 million** transactions worth over **$600 million**

As digital transformation has evolved, so has the convenience of paying for goods and services. Seamless, frictionless payments have become an essential part of our everyday lives, often happening behind the scenes without any interaction with the consumer. Billions of payments are taking place daily, and consumers trust that their payments will be successful every time, whether paying a bill, picking up a prescription or tapping in and out of the turnstile.

Along with the digital transformation, however, has come increased risk to the promise of frictionless 'always on' payment capabilities as new threats have emerged. For financial institutions, these can come in many forms, from the rise in cyberattacks, which bring more challenges, to the constantly evolving regulations, which demand compliance.

Additionally, as banks increasingly rely on third-party providers to enhance their networks, they create new dependencies that can result in more points of risk, as well as operational failure.

When these risks lead to outages, they have the potential to cause massive disruption, jeopardising consumer trust.

Don't wait until it's too late

Measures taken years ago may no longer be sufficient to protect financial institutions from threats today and in the future. It is more critical than ever that banks ensure that their systems are resilient.

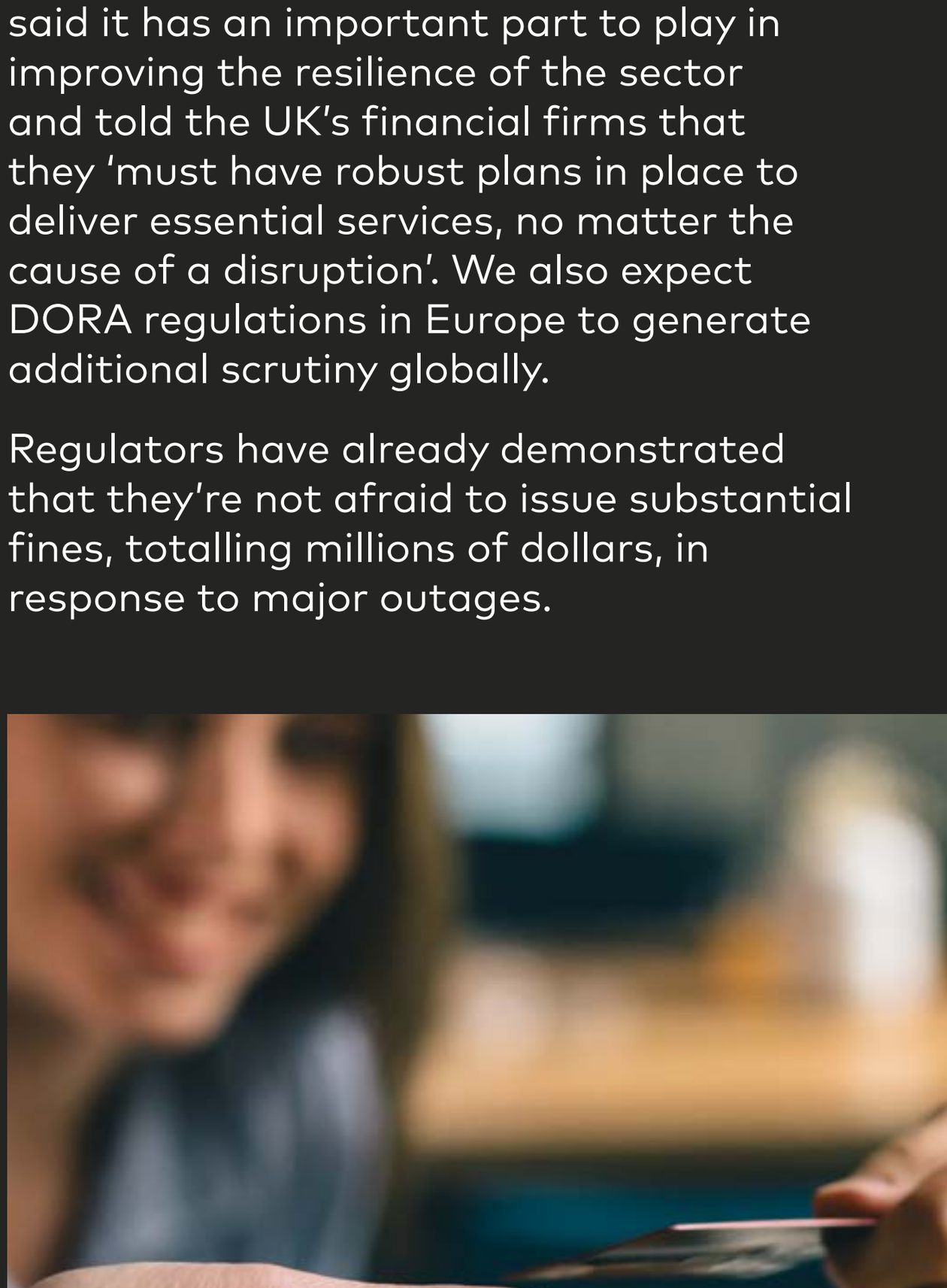
For those that have fallen victim to a major outage, this will not be a message that needs to be heard twice. In addition to the reputational harm resulting from a network failure, the financial cost can be damaging as well. In one recent example, an issuer with an ill-prepared resiliency capability declined, over the course of several hours, more than 14 million transactions, worth over $600 million.

Regulatory pressure is rising

Given the level of consumer disruption that outages have caused in recent years, regulators are increasingly interested in how financial institutions are building resiliency into their payment systems.

Earlier this year, the Bank of England said it has an important part to play in improving the resilience of the sector and told the UK's financial firms that they 'must have robust plans in place to deliver essential services, no matter the cause of a disruption'. We also expect DORA regulations in Europe to generate additional scrutiny globally.

Regulators have already demonstrated that they're not afraid to issue substantial fines, totalling millions of dollars, in response to major outages.



With the threat of an incident always a possibility, this is not something that can be left to chance. So when assessing the landscape for risks — be they from cyberattacks or technology failures — the mantra is the same: Build resilience now to avoid disruption tomorrow.

Building resilience through technology

As the landscape has changed, what was considered resilient yesterday may be vulnerable today. At Mastercard, we have continued to evolve our technology to keep payments secure.

As part of our network promise, Mastercard provides robust resiliency capabilities by decisioning transactions for issuers in the event of an outage. This allows issuers to focus on fixing the problem and minimising the disruption experienced by their cardholders.

As a matter of fact, an average of 1,200 issuers rely on this capability each day.

Driving consumer trust

Resiliency is the key to securing consumer trust. With the right solutions in place, consumers can be confident that they will not be left stranded, even when things go wrong behind the scenes.

And that's where Mastercard's suite of payment resiliency solutions comes in. It can assist banks with timely and accurate on-behalf decisioning of authorisation requests — ultimately protecting their brand and reputation and, most importantly, ensuring a frictionless cardholder experience.

How telecom providers stay ahead of third-party risk

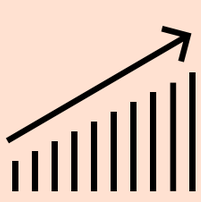
Paul Trueman
Executive Vice President, Segment Intelligence and Engagement

More innovation, more complexity

The telecommunications industry is evolving and growing at an exponential rate, with revenues projected to rise 6.2% annually through 2030[32]. This surge comes from a multitude of new offerings — new entertainment and data services, financial solutions, gaming and virtual reality, identity and home security, advertising and other offerings — many of which are brought to market in partnership with other providers and third-party vendors.

The rapid pace of advancement can expose the network to new security risks and vulnerabilities. For example, the growth in 5G is driving IoT connections and new players into the digital ecosystem, contributing to a rise in threats and vulnerabilities. Bad actors require only one weak link in a vendor network to threaten the entire ecosystem.

Telecoms is one of the sectors most exposed to attack. As a leading player in the digital ecosystem, it is vital that telecoms are resourced to counter the rising number of threats.



Healthy growth...

6.2%

The global telecom services market is expected to grow 6.2% annually through 2030, from $1.8 trillion in 2022[33]

But rising attacks...

50%

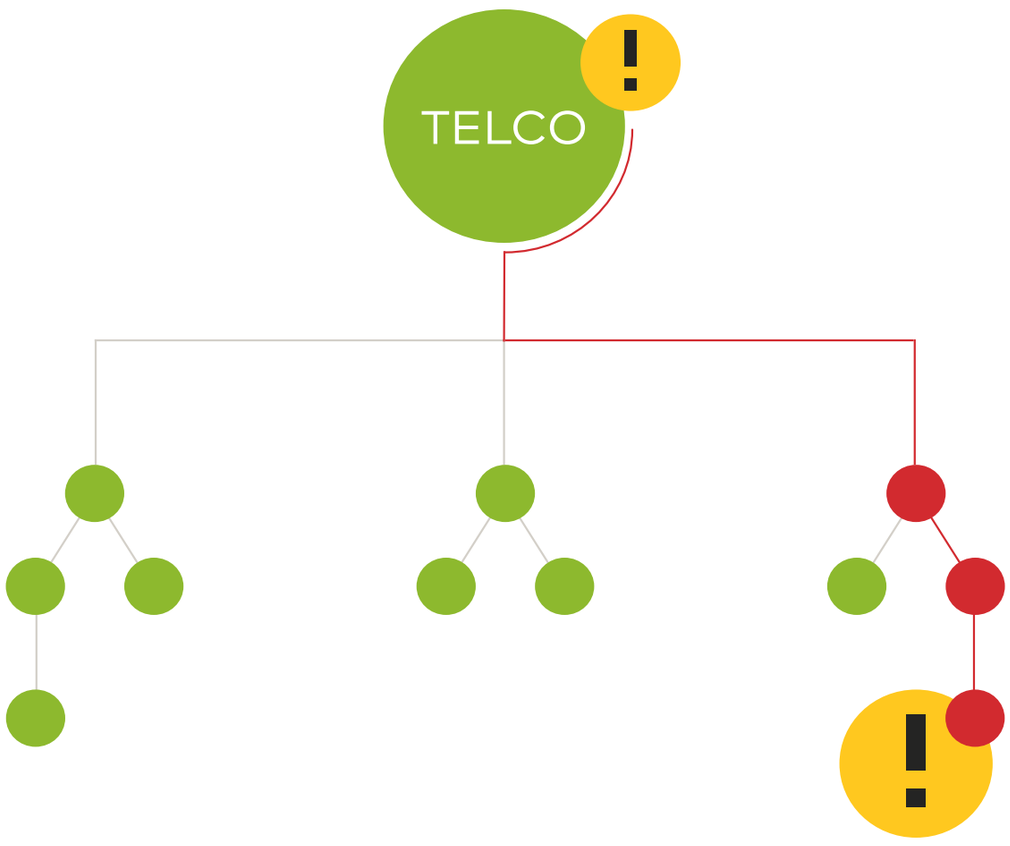
Cyberattacks on corporate networks rose 50% in 2021, and the communications industry ranked third[34] in attacks overall

Equals greater fraud

$39.9B

The global telecoms industry lost an estimated $39.9 billion to fraud in 2021[35]

A growing network opens the door to more opportunities for fraud and cyber attacks



The dimensions of fraud

Many factors contribute to the growing fraud risk for the telecommunications industry. Some are widespread and affect all industries, such as the burgeoning rise in social engineering schemes, phishing and pharming. Others affect telecoms more directly, particularly with the proliferation of mobile device usage. These include:

- Impersonation with stolen credentials
- An increase in stolen equipment
- Attacks on telecoms suppliers, partners and vendors

Not only are these risks costly to telecoms, they also harm customers who have little patience for risk from their telecommunications providers. In fact, nearly three out of four US consumers (73%) say they will walk away from a brand after only one poor customer service experience.[36] This risk to brand reputation and customer loyalty, along with fraud, extends to partners and other stakeholders in the value chain, such as financial services and entertainment companies.

> 'Exponential growth in demand for telecommunications services brings with it exponential risks and threats. And the impact of these threats is felt by every stakeholder: the consumer, telecoms, financial services and other industries. Only an end-to-end, 360-degree approach can secure the ecosystem and sustain this growth'.

	FOCUS AREAS	RECOMMENDATIONS
Growing ecosystem	**As telecoms offer more services through acquisitions, vendors and third parties, they face:** • Rising cyber risks from third parties • Increasing exposure of customer data via external services such as banking, entertainment, etc.	**Cyber risk management solutions can help telecoms:** • Gain visibility into cyber vulnerabilities, as well as risk exposure from third-party partners • Protect financial ecosystem partners (banks, insurance companies, etc.)
Onboarding entities and individuals	**Effortless onboarding of innovative services is essential to both telecoms suppliers and customers:** • Telecoms rely on numerous providers to deliver the services that consumers demand in their digital ecosystem • Onboarding agents, merchants, partners and individuals in a secure and cost-effective manner is a major effort	**Systemic risk management solutions can help telecoms:** • Check consumer financial credit risk • Reduce merchant onboarding risks as well as ongoing risk at the merchant and transaction level, while increasing approval rates • Fully vet the risk when establishing new business relationships
Authentication	**As consumers use their mobile devices more often for more services:** • They can get frustrated if their user experience isn't seamless across the customer journey • They worry that their reliance on mobile devices exposes them to identity and account theft	**Account opening and management solutions can help telecoms:** • Proactively manage account continuity and effectively authenticate payment data • Deploy behavioural analytics to evaluate a customer's identity and ensure a frictionless experience

Key takeaways

The telecommunications industry is enjoying continued growth as consumers embrace the always-on convenience of a mobile lifestyle. Yet with that growth comes many new challenges to the industry. Telecoms can seize this opportunity to incorporate innovative new services that transform the user experience, deepen customer engagement and loyalty, and ensure confidence in the security of customer data while simultaneously lowering costs and increasing revenue. Choosing the right technology partner to do so is critical.

Mastercard, a widely recognised technology innovator, has the proven technology, deep industry experience and commitment to help telecoms:

- **Optimise their business:**
  Seamlessly implement new services to increase revenue while reducing operating and capital costs

- **Enhance customer journeys:**
  Improve the user experience and customer journey at every interaction

- **Mitigate fraud:**
  Secure digital identities, resist cyberattacks and authenticate users and devices end to end

Mitigate cyber threats within your organisation and across your business relationships

Mastercard's third-party risk management capabilities provide continuous cyber risk monitoring of your third-party and extended supply chain. This approach allows you to preemptively identify, prioritise and reduce risk.

As a leading provider of cybersecurity ratings and insights, we are...[37]

Trusted by
21,500+
global users

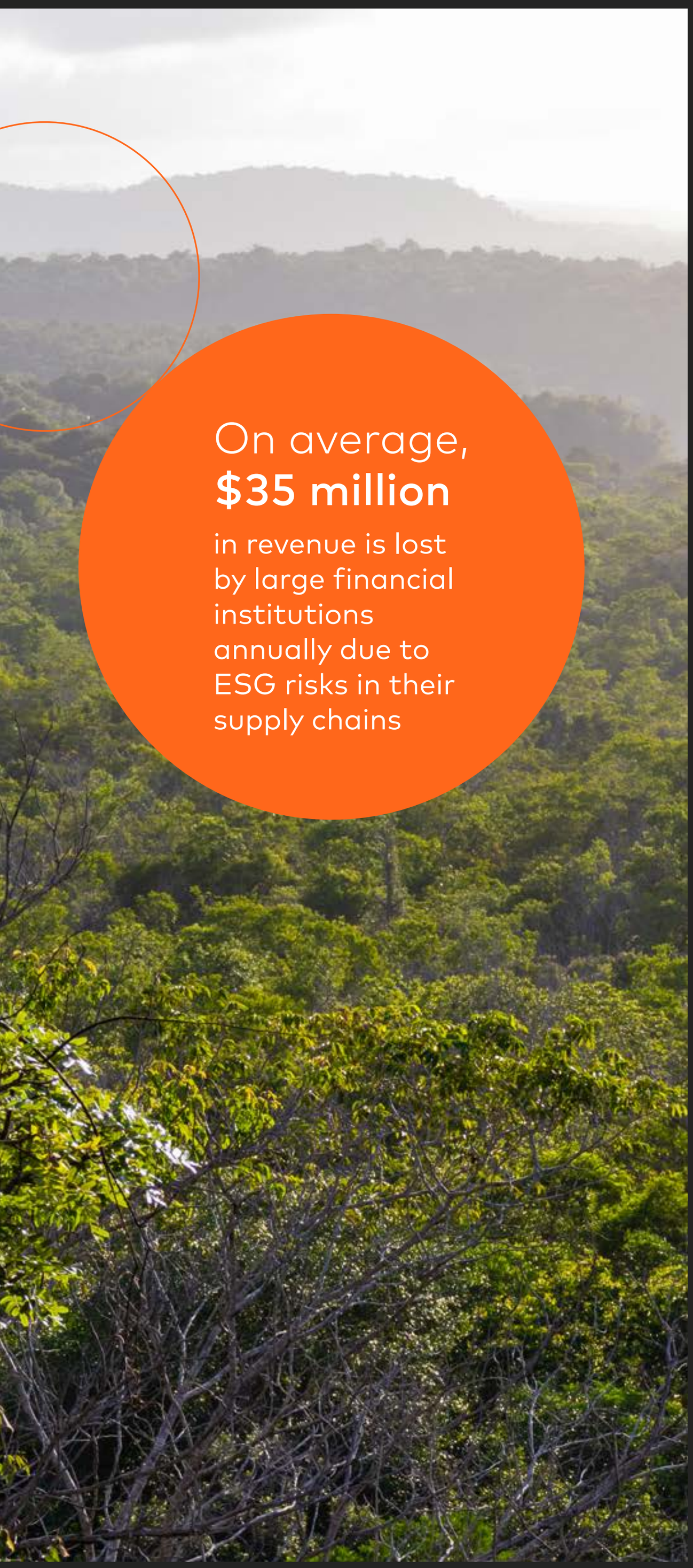
Supporting
30+
industries

Monitoring
19+
million companies

Fostering
97%
annual customer retention rate. Gartner Peer Review rated 4.4 out of 5 stars

Companies can no longer ignore ESG risks

Johan Gerber
Executive Vice President, Security and Cyber Innovation



Managing environmental, social and governance (ESG) risks has become increasingly important for financial institutions that want to stay competitive. We partnered with Interos to conduct a study of ESG scores from 1,533 North American and 556 European financial institutions (FIs) to look at the impact these practices can have on businesses' cyber, financial and operational risks.

Addressing ESG risks — risks related to how a business impacts the environment, treats security and employees and governs itself — is crucial because these risks can, and do, result in lost money, opportunities, customers and employees. It's important to remember that ESG covers a broad range of activities, including ethical business practices, compliance, workplace safety and fair pay, as well as climate change and sustainability. It's this range that makes ESG such an important key performance indicator.

ESG management is important to all stakeholders

A recent study from Interos found that large financial institutions lose an average of $35 million in revenue annually due to ESG risks in their supply chains, including climate change, counterfeit exports and modern slavery.[38]

Looking at ESG risks has become mission-critical for companies, especially in the past few years as the frequency of large-scale disruptions has increased. Events that were previously thought of as rare have become more commonplace, such as severe weather events.

Meanwhile, ESG is important to investors, too. They consider how companies are performing on ESG when they make their funding decisions.

Employees and customers report that they also want businesses to increase their ESG efforts.

In a 2021 PwC study, two out of three Americans said their social values influence their shopping choices. The study found that **76% to 86% of employees and customers are more likely to work for or buy from companies that stand up for the environment, social causes and governance.**[39] Some 83% of those surveyed believe that companies should actively shape ESG best practices.[40]

Regulations tightening

At the same time, ESG compliance requirements worldwide are only intensifying. Earlier this year, the US Securities and Exchange Commission proposed a rule requiring public companies to provide detailed reporting of their climate-related risks, emissions and net-zero transition plans.[41]

In Europe, Germany enacted a law requiring all companies with more than 1,000 employees doing business within the region to identify human rights violations and environmental risks within their supply chains.[42]

Other governments around the globe are implementing ESG regulations, too, and more than 120 companies now report their ESG metrics as part of the World Economic Forum's Stakeholder Capitalism Metrics.[43]

Financial institutions slow to adjust to an ESG world

Yet despite these compelling reasons to put more resources toward ESG risk, financial institutions in both North America and the European Union have been slow to make these types of risks a priority.

Interos found that, on average, European and North American financial institutions have medium ESG risk scores, whereas their financial and cyber risk scores typically fall into the low-risk category.

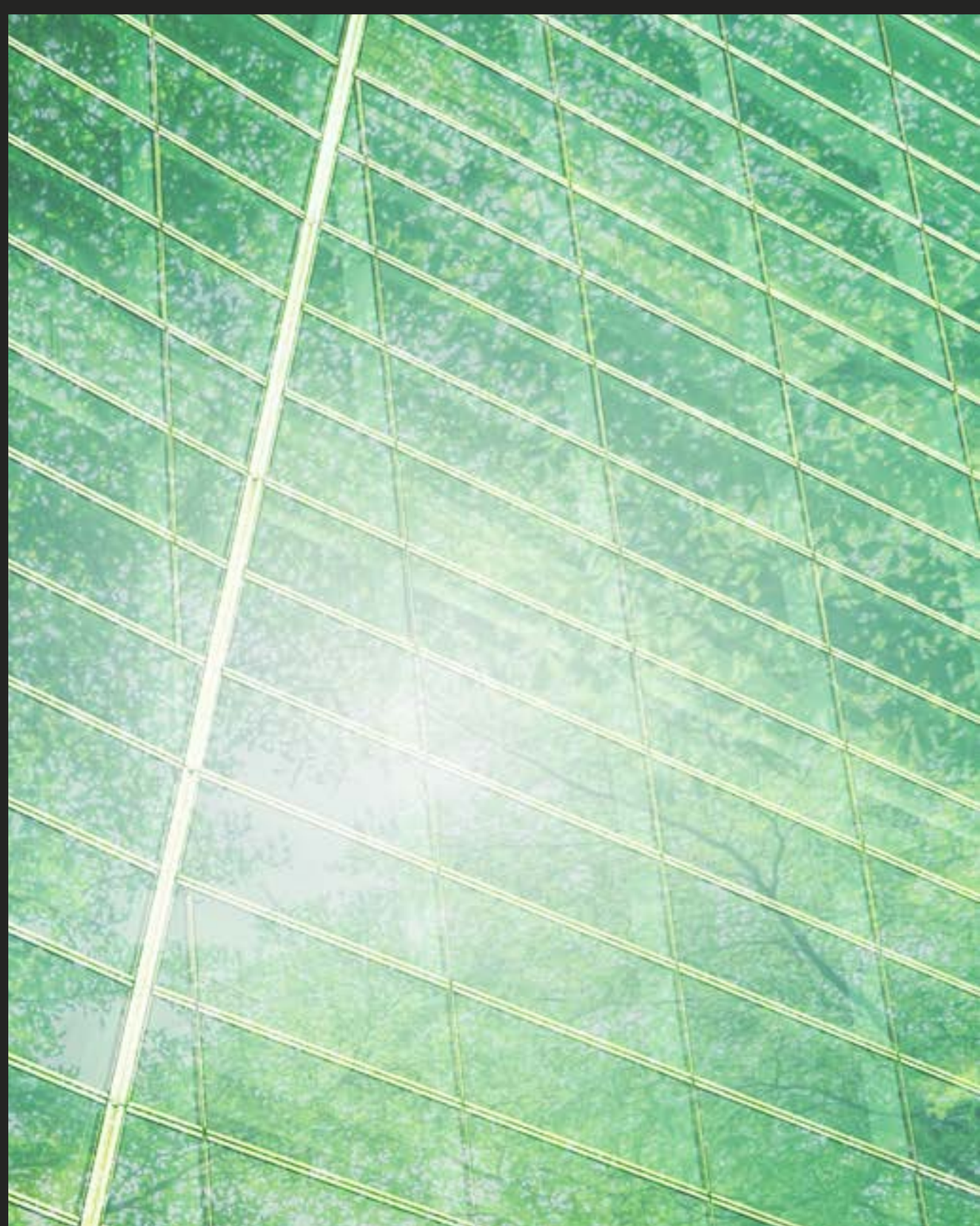
Banks have historically worried less about ESG risks in part because ESG mandates are not strict regulatory mandates with financial repercussions in all jurisdictions. What's more, the definition of ESG can be confusing and a gold standard hard to define. Finally, ESG is a relatively new risk factor — a lot of financial institutions just haven't caught up.

Other institutions have acted, but they've focused mostly on the 'E' (environmental) aspect of ESG risk, with a light touch or focus on social and governance, despite the fact that about 1,400 academic studies found a positive relationship between ESG scores and financial returns.[44]

Lowering ESG risk

Overall, financial institutions could do a better job managing ESG within their supply chains by exploring ESG risks in greater depth. To be effective, banks can no longer rely solely on legacy methods such as credit risk ratings that provide a perspective of risk in relatively narrow financial terms — this will likely be insufficient as regulators demand greater transparency in the name of a more sustainable future.

Financial institutions need better, more holistic tools that can help them effectively manage these growing ESG risks. A comprehensive solution, such as Mastercard Systemic Risk Assessment, can help banks identify and minimise business, supply chain and ESG risks and give financial institutions a true competitive edge.[45]



riskX

Come to Barcelona!

Join us at the W Hotel in Barcelona on October 23-26, 2023 to connect with global tech leaders and industry peers as we discuss the forces reshaping today's digital economy — and your business.

Steven Bartlett

Entrepreneur, speaker, investor, bestselling author and the host of UK's No. 1 Podcast 'The Diary of a CEO'

Angela Oguntala

Founding Partner, Greyspace

Mike Walsh

CEO, Tomorrow

Georgie Barrat

'Gadget Show' presenter and tech journalist

Bryan Habana

Mastercard Global Ambassador & South African rugby legend

Get ready to learn how advances in identity verification can unlock more superior and far more secure customer experiences. Discover the impact of new AI technologies in the payments ecosystem and gain insights on how to protect your business and customers from fast-evolving fraudsters and cybercriminals. This event is specifically designed for decision makers and leaders in the areas of cyber, fraud, crypto, security, risk, operations and technology.

Register here:

mastercardriskx.cventevents.com

Notes

ARTIFICIAL INTELLIGENCE

1 United Nations Office on Drugs and Crime, 2023.

2 Juniper Research, 'Emerging Trends, Regulatory Impact & Market Forecasts 2022-2026'.

3 'Global Anti-Money Laundering Fines Surge 50%', Financial Times, 18 January, 2023. >

4 Capgemini, World Payments Report 2022. >

5 Michael Chui, Eric Hazan, Roger Roberts, et al, The Economic Potential of Generative AI: The Next Productivity Frontier (McKinsey, 2023). >

6 Oyku Isik and Lisa Simone Duke, Mastercard's Ethical Approach to Governing AI (Harvard Business Publishing, 2022). >

7 AI perspectives: Transaction fraud >

8 The potential impact of Artificial Intelligence in the Middle East - PwC Middle East >

IDENTITY

9 Fenergo, 'KYC compliance for banks: Addressing the cost', 10 January 2023. >

CYBER

10 Dorothy Pomerantz, 'A Perfect Mate, or a Perfect Mark? How People Become Victim to Online Romance Fraud', Mastercard Newsroom, 12 May, 2021. >

11 UK Finance, Annual Fraud Report: The Definitive Overview of Payment Industry Fraud in 2022. >

12 ACI Worldwide and GlobalData, Growth in APP Scams Expected to Double by 2026, Business Wire. >

13 UK Finance, Annual Fraud Report: The Definitive Overview of Payment Industry Fraud in 2022. >

14 Ibid.

15 Ethoca, Digital Field Guide: What Consumers Want From Digital Banking (Mastercard, 2023). >

16 John Horn, Aite-Novarica, 2023.

17 Ethoca, Digital Field Guide.

18 Ibid.

19 Ibid.

20 CoinGecko, Global Cryptocurrency Market Cap Charts. >

21 FATF regional bodies promote similar issues of money-laundering prevention, etc., within regions.

22 Fiat money (e.g. US dollars, Euros) is a currency that is declared as legal tender by a government decree but has no intrinsic value and is not backed by any tangible asset, e.g. gold or silver.

23 RiskRecon, 'Vulnerability in Cybersecurity: Finding and Fixing Your Cyberspace's Weak Points', 8 May, 2023. >

24 RiskRecon, 'Balancing Third-Party Risk: Taking Time to Calibrate', 21 June, 2023.

CYBER (CONTINUED)

25 RiskRecon, 'Cybersecurity Trends: How to Stay on Top of Them', 6 May, 2023. >

26 RiskRecon, 'Cybersecurity Service: Helping Your Company Protect Its Cybersecurity Assets', 7 May, 2023. >

27 RiskRecon, 'The Enterprise Risk Management Framework', 3 July, 2023. >

28 RiskRecon, 'Security Risk Assessments and Why Your System Needs Them', 7 July, 2023. >

29 RiskRecon, 'What Is a Risk Management Framework?', 4 May, 2023. >

30 RiskRecon, 'Cybersecurity Frameworks, Explained', 28 June, 2023. >

31 RiskRecon, 'Enterprise Cybersecurity: Keeping Your Business Safe in Cyberspace', 5 July, 2023. >

RISK & RESILIENCY

32 Grand View Research, Telecom Services Market Size, Share & Trends Analysis Report By Service Type, By Transmission, By End-use, By Region, And Segment Forecasts, 2023–2030.

33 Casey Herman, PwC, 'How much does the public care about ESG?', 2022.

34 U.S. Securities and Exchange Commission, 'SEC proposes to enhance disclosures by certain investment advisers and investment companies about ESG investment practices', 25 May 2022.

35 Library of Congress, 'Germany: New law obligates companies to establish due diligence procedures in global supply chains to safeguard human rights and the environment', 17 August 2021.

36 World Economic Forum, 'Stakeholder Metrics Initiative: Over 120 companies implement the ESG reporting metrics', 9 January 2023.

37 McKinsey, 'Why ESG is here to stay', 26 May 2020.

38 Grand View Research, Telecom Services Market Size, Share & Trends Analysis Report By Service Type, By Transmission, By End-use, By Region, And Segment Forecasts, 2023–2030.

39 Check Point Research, '2022 Security Report', 21 January 2022.

40 Communications Fraud Control Association, 'Fraud Loss Survey Report 2021'.

41 TCN, 'Consumer Insights About Customer Service Survey', 2023.

42 RiskRecon, 2023.

43 Interos, 'Resilience 2022: Interos Annual Global Supply Chain Report', 11 May 2022.

44 PwC, 'Beyond compliance: Consumers and employees want businesses to do more on ESG', 2021.

45 ESG and a rapidly evolving risk climate >

For more information visit:

b2b.mastercard.com/

Or contact your Mastercard representative.

LinkedIn