A MASTERCARD MARKET INTELLIGENCE REPORT: FINANCIAL INSTITUTIONS AND MERCHANTS, NAM

Delivering Intelligent Authentication

Why a multi-layered security strategy supported by connected intelligence is critical to secure today's digital ecosystem

mastercard

Table of contents

This document includes interactive features to help you navigate. Use ➔ above to access different sections of the report.
Click the ⌂ icon on the top-right corner of each page to return to this page.

Executive summary

Consumers' merging digital and physical interactions open the door to new opportunities—and new challenges

Consumers are changing how they shop, travel, pay, and connect—blurring the boundaries between physical and digital. From tapping to pay with a digital wallet to logging in to a mobile banking app, consumers expect their digital experiences to be simple, convenient, and secure. The speed at which digital commerce is growing is proof that consumers seek a richer, more consistent user experience (UX), no matter where, when, and how they engage with their financial institution and merchants.

Unlike payments in the physical world, however—where 98% of transactions are approved in the U.S.[1] and fraud is low—card-not-present transactions are plagued by unnecessary friction, uncertainty during checkout, and growing fraud. As EMV chip cards bring greater security to the physical point-of-sale, fraudsters are turning their efforts to card-not-present transactions—which now represent 59% of all fraud, even though they are only 22% of purchase volume today.[2]

As fraud becomes more sophisticated, balancing an optimized UX against strong authentication is increasingly difficult. A strong, multi-layered security strategy that continually learns from a growing store of transaction, geolocation, biometric, device, and other data, can help financial institutions and merchants outsmart the fraudsters. Intelligently connecting the various sources of data to drive meaningful insights and impact becomes the key to deliver the simplicity and seamless experiences consumers demand, while keeping your business safe, even as fraud continues to evolve.

As digital touch points rise, consumer expectations of simplicity, convenience, and security do as well.

400B

Nearly 400 billion interactions with online environments worldwide in 2018[3]

↑ 60%

U.S. digital commerce sales will increase by 60% between 2019 and 2022[4]

But as interactions move digital, so too does the growing threat of fraud.

28%

of the 400 billion online interactions worldwide were high-risk events[3]

90%

Up to 90% of all login traffic to global retailers in 2017 were actually hackers using stolen data[5]

[1] Mastercard, Oct 2017–Sep 2018 data, across all card types, 2018.

[2] Federal Reserve, Payments Study: Annual Supplement, 2017.

[3] NuData Internal Analytics, 2018.

[4] eMarketer, Feb 2019. Total retail excludes travel and event tickets.

[5] Shape, 2018 Credential Spill Report.

State of the market

As consumers' preferences shift to digital, it becomes difficult—and critical—to connect the fragmented set of data for a holistic view of the customer

Throughout each day, people shift their attention from one device to the next: from laptop to smartphone, from tablet to smartwatch, as well as a growing number of IoT devices.

These new points of interaction add complexity and vulnerability to the digital ecosystem, including payments. Fraud traditionally migrates toward the weakest point in the system. So it is no surprise that cybercrime continues to escalate in the ecommerce space—making it highly vulnerable. In fact, digital fraud has taken on multiple new forms: from account takeovers and identity theft to loyalty fraud and new account fraud.

But simply applying legacy security measures to new use cases won't work either. Indeed, when consumers are falsely declined, not only is revenue lost, but the experience can seriously erode loyalty—pushing many consumers to abandon the financial institution or merchant connected with the erroneous decline. As more consumers make more card-not-present transactions, these false declines are becoming dangerously common, and immensely expensive.

Identity verification is a top challenge facing financial institutions and merchants[1]

Connected intelligence, a multi-layered security strategy

As mobile, in-app, and IoT payments continue to grow, financial institutions and merchants must stitch together an increasingly fragmented dataset during authentication to keep growing their business without consumer disruption or losing share to competitors. A multi-layered approach to security that can deliver connected intelligence—thousands of data points and hundreds of decision points throughout the customer journey, evaluated by a coordinated set of AI-based services—can help ensure that the consumer is not only protected, but that financial institutions' and merchants' own environments are not compromised during a transaction.

[1] LexisNexis, 2018 True Cost of Fraud Study, Aug 2018.

Urgency

Fraudsters are finding creative ways in into financial institutions' and merchants' digital environments

Without a proper multi-layered, connected approach to security, you are leaving yourself and your consumers vulnerable to sophisticated and quickly evolving fraudulent activity, as well as potentially declining legitimate transactions. Both will negatively impact your business. Examples of how your business could be vulnerable include:

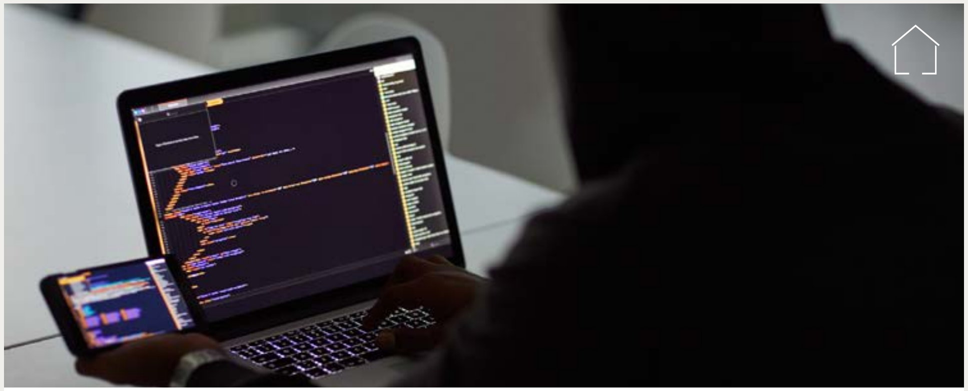
- **Account takeover** – when a good user's account is literally taken over by bad actors, often as a result of continuously evolving automated scripts. Usually carried out by bots, and takes the form of credential stuffing or credential cracking.

- **Identity theft** – when a consumer's identity is used by bad actors for malicious purposes, such as opening credit lines or purchasing big box items using legitimate credentials.

- **Loyalty fraud** – when bad actors are able to take over an account and then use hard-earned loyalty points or rewards to benefit themselves.

- **False declines** – declining legitimate transactions from good consumers is a sign that inadequate authentication measures are in place, possibly costing the business significant revenue opportunities.

While each of these threats can be mitigated separately, financial institutions and merchants don't always have all the appropriate measures in place for a holistic picture.



Rising fraud is driving up costs and false declines are eroding trust and revenue

$200B

are lost in retail sales each year in the U.S. due to friction at checkout[1]

44%

of declined consumers stopped or reduced shopping with retailer[3]

$3.27

Every $1 of fraud costs financial institutions and mid-large retailers an average of $3.27[4]

51%

of declined consumers used another card to complete purchase after being falsely declined[3]

[1] PYMNTS.com, Checkout Conversion Index, data for Q2 2017, 2018.
[2] Federal Reserve. Payments Study: Annual Supplement, 2017.
[3] Javelin Advisory Services, Addressing the Threat of False Positive Declines, Oct 2018.
[4] FIs with mCommerce and mostly digital transactions, Merchants with mCommerce and selling digital goods. LexisNexis, True Cost of Fraud Study, 2018.

Opportunity

The benefits of multi-layer security can be easily quantified for financial institutions and merchants

For financial institutions and merchants to truly secure their digital environments to drive revenue, security solutions have to address the challenges across all digital channels and use cases, including logging in to your mobile banking app or merchant app, financial institution website or merchant website, or even when creating a new account.

And while a multi-channel and multi-layered strategy is critical, it is only beneficial if it addresses the top challenges facing financial institutions and merchants today:

- Reduce fraud by stopping bad actors before and during checkout
- Reduce false declines and approve good users
- Reduce the threat of account takeover and automated attacks
- Increase approvals and thus shopping cart conversion
- Improve the consumer experience from shopping cart to payment
- Increase operational efficiencies from reduced fraud activity and customer service calls

Stronger authentication and security measures can help balance an optimized user experience with reduced fraud. When billions of data points are harnessed from different customer interactions and examined with AI and machine learning, you can seamlessly connect the dots and gain a holistic picture of the user. This manifests in a seamless consumer experience and gives consumers the sense of security, trust, and convenience they want from digital interactions.

Richer data exchanged between merchant and financial institution, biometrics, artificial intelligence, and other tools provide more accurate assessments of fraud risk

10x

more data shared by merchants during EMV 3DS authentication enhances financial institutions' approval decisions

>10K

State-of-the-art AI can process tens of thousands of transactions per second

Intelligent authentication increases approvals, even as it reduces fraud

↑12%

potential lift in approvals, when transactions in North America are fully authenticated[1]

<12BPS

lower digital fraud when transactions in North America are fully authenticated[2]

[1] Mastercard, North America data Oct 2017–Sep 2018, across all card types.

[2] Mastercard Q2 2018 data across all card types – average reduction in fraud with fully authenticated transactions.

Implications

As stakeholders face margin pressures, security can be a driver of differentiation and consumer loyalty

1. **Put the consumer at the center** – To provide consumers the convenience and simplicity they demand at every point-of-interaction, authentication is moving from passwords they frequently forget to stronger forms of authentication. Armed with greater data and intelligence, financial institutions and merchants can offer a seamless experience that is nearly invisible to the consumer.

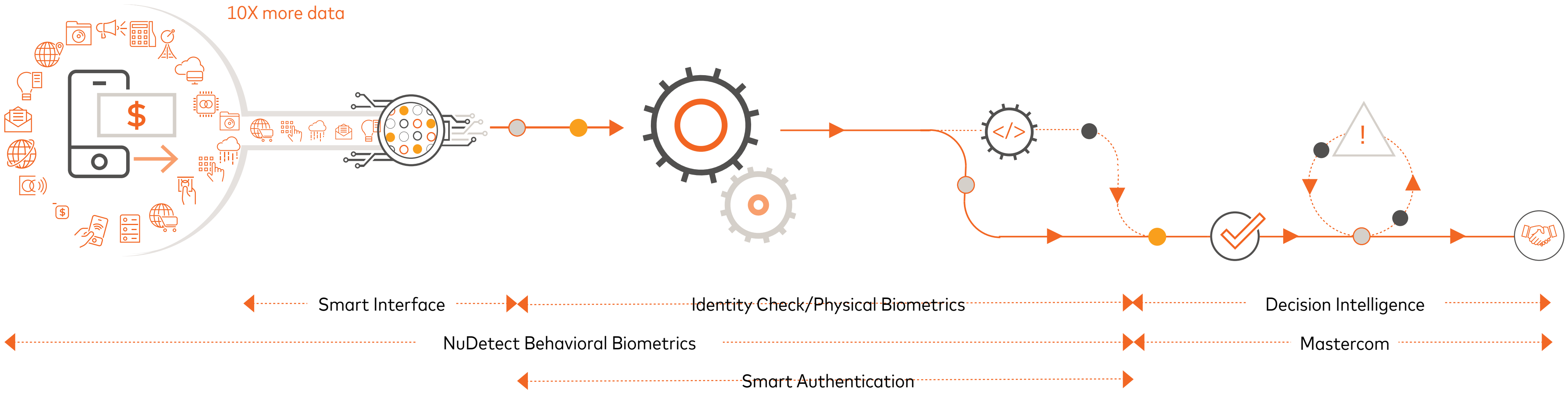
2. **Synchronize security across the user journey** – Most organizations are using non-standardized security methods by channel and type of interaction, defined in silos by different areas of the company. Consumers will be more satisfied and loyal if they enjoy the same user experience whether visiting a bank branch, using an ATM, banking online, making a purchase in the physical or digital domain, or seeking customer service.

3. **Protect your digital ecosystem** – The key to staying ahead of fraudsters is to proactively secure your digital web and mobile channels with cutting-edge security technology. Machine learning continually learns from billions of transactions and behavioral events to enhance scoring. APIs provide the flexibility to add new services in response to the changing fraud landscape and evolving business goals.

4. **Take advantage of new industry protocols** – Leverage the EMV 3-D Secure 2.0 protocol to share more data with stakeholders, such as consumer account, device, and other valuable information. Risk-based authentication silently eliminates unnecessary friction on low-risk transactions to help drive greater security, profitability, and an optimal user experience.

Multi-layered Connected Intelligence

Mastercard delivers strong security with low friction throughout the consumer journey. And because our systems continuously learn from every transaction and continually grow more intelligent, accuracy rises over time.



10X more data

Smart Interface

Identity Check/Physical Biometrics

Decision Intelligence

NuDetect Behavioral Biometrics

Mastercom

Smart Authentication

Access Account Checkout Authentication Verification Authorization Dispute

Monitor behavioral interactions of the consumer and account accessing the ecosystem

ENGAGEMENT

Review consumer attributes and payment credentials and verify their identity

IDENTIFICATION

Score fraud risk using enhanced AI models, advanced data insights, and rules

DECISIONING

Mastercard's multi-layered, connected intelligence begins as the customer interacts with their device or account and increases along each step of the customer journey.

Leveraging thousands of unique data points and hundreds of decision points throughout the customer journey, as well as our coordinated set of AI-based solutions and machine learning tools, we help financial institutions and merchants deliver a more secure digital ecosystem and a seamless user experience that is nearly invisible to the consumer.

Outcomes

Mitigate fraud and enhance the user experience—in commerce, loyalty, and operations—without increasing risk

Reduce CNP fraud

By facilitating the exchange of consumer and device data provided through the EMV 3-D Secure protocol—such as account, device, and IP address, for example—stronger authentication with Mastercard provides financial institutions a level of assurance that they are authorizing a payment from the right consumers.

Virtually eliminate account takeover attacks

By starting the authentication process even before a customer logs in to your environment, you can keep your business and your customers safe from bots and other emerging threats. The first layer in a multi-layered approach to security includes pre-authentication solutions that block automated attacks such as account takeover with +99% accuracy.

Deliver a positive consumer experience

With multi-dimensional, data-driven criteria applied in real-time—such as amount, location, channel, transaction type—Mastercard can help financial institutions approve more genuine transactions without adding any friction to the consumer journey in the majority of transactions. This can ensure an interruption-free shopping experience, potentially leading to greater loyalty from high-value customer segments.

Leverage new technology and industry standards

By leveraging the holistic security solutions of Mastercard—advanced technologies like biometrics, risk-based authentication, and artificial intelligence—financial institutions and merchants can enhance their decisioning performance while reducing their IT investment in fraud management.

↑ 5%

Fully authenticated ecommerce transactions have 5% higher approval rates than non-authenticated transactions[1]

↓ 50%

Mastercard helped a financial institution that was declining high-spending debit cardholders at twice the rate of other segments reduce false declines by 50%, without increasing risk exposure[2]

↓ 50%

Real-time risk scoring, powered by machine learning, could help a financial institution with an annual GDV of $12B and fraud losses of $12M (10 bps), reduce false positives by 50% while identifying 19% more fraud[3]

>99%

Combining Mastercard behavioral biometrics with device intelligence and user analytics, automated fraud attacks from bots are detected with +99% accuracy[4]

[1] Mastercard, 2017 data across all card types.
[2] Mastercard, NuData results.
[3] Mastercard. global model performance results, 2017.
[4] Mastercard, internal analytics.

Key takeaways

1 **Consumers want simplicity and security** in every interaction with their favorite brands—financial institutions, merchants, and throughout their connected lives—regardless of which device or channel they use. To meet the demand for a seamless consumer journey, financial institutions and merchants must intelligently assess risk to reduce the need for unnecessary friction, enhance decisioning, and optimize the consumer experience.

2 **A layered approach to security** is necessary to meet the evolving behaviors and needs of consumers, as well as to address the increasing complexity of fraud. In addition to technological challenges, more than half of identity and authentication decision makers at U.S. businesses believe their authentication methods will not be sufficient to meet regulatory standards in a few years. Standardized process controls integrated across all customer touchpoints are key to providing a secure and frictionless environment—before, during, and after the transaction.

3 **False declines are causing more damage than fraud** – While consumers worry about security, they are equally frustrated by being falsely declined. Not only do merchants lose a sale, but they are likely to lose a customer. And that stymied cardholder is also likely to abandon the issuer of the declined card. Advanced authentication tools, like biometrics, can reduce these declines while boosting security.

4 **Fraud of the future requires security solutions of the future** – As the number of devices, channels, and amount of data all multiply, security is lagging behind digital innovation. And with more sophisticated fraud, cyberattacks, data breaches, and identity theft are on the rise. Only by securing the entire ecosystem with multichannel, intelligent security solutions across all customer touch points can we defeat fraud as it evolves.

For more information on Mastercard® security solutions, please contact your account representative or visit www.mastercard.com/authentication.

mastercard.

This document is proprietary to Mastercard and shall not be disclosed or passed on to any person or be reproduced, copied, distributed, referenced, disclosed, or published in whole or in part without the prior written consent of Mastercard. Any estimates, projections, and information contained herein have been obtained from public sources or are based upon estimates and projections and involve numerous and significant subjective determinations, and there is no assurance that such estimates and projections will be realized. No representation or warranty, express or implied, is made as to the accuracy and completeness of such information, and nothing contained herein is or shall be relied upon as a representation, whether as to the past, the present, or the future.