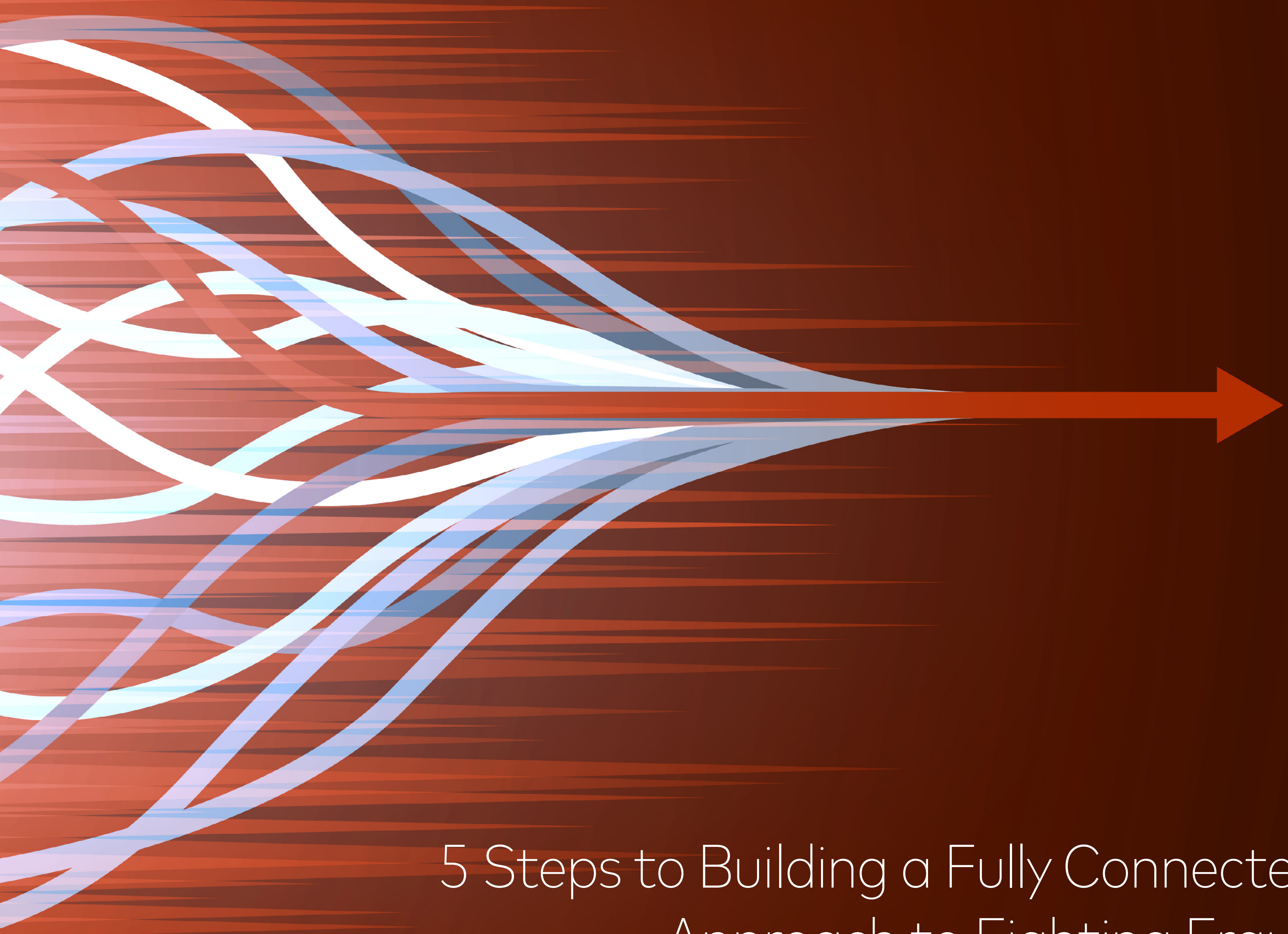


>>

5 Steps to Building a Fully Connected Approach to Fighting Fraud

While Improving the User Experience

As digital commerce in the U.S. grows three times faster than all other retail sales[1], criminals are employing ever-more sophisticated tools to exploit every point of weakness throughout the consumer journey. The threat is very real: fraud in digital commerce is four times the rate of fraud at the physical point of sale, while representing only a fraction of total transaction volume. Responding to the rise in fraud through digital channels, too many issuers and merchants are overcompensating by dialing up their existing fraud criteria and flagging suspicious transactions as fraudulent. Yet many of the transactions they are declining are genuine. U.S. merchants are expected to lose $443 billion in revenue due to false declines in 2021—up 34% from $331 billion in losses in 2018.

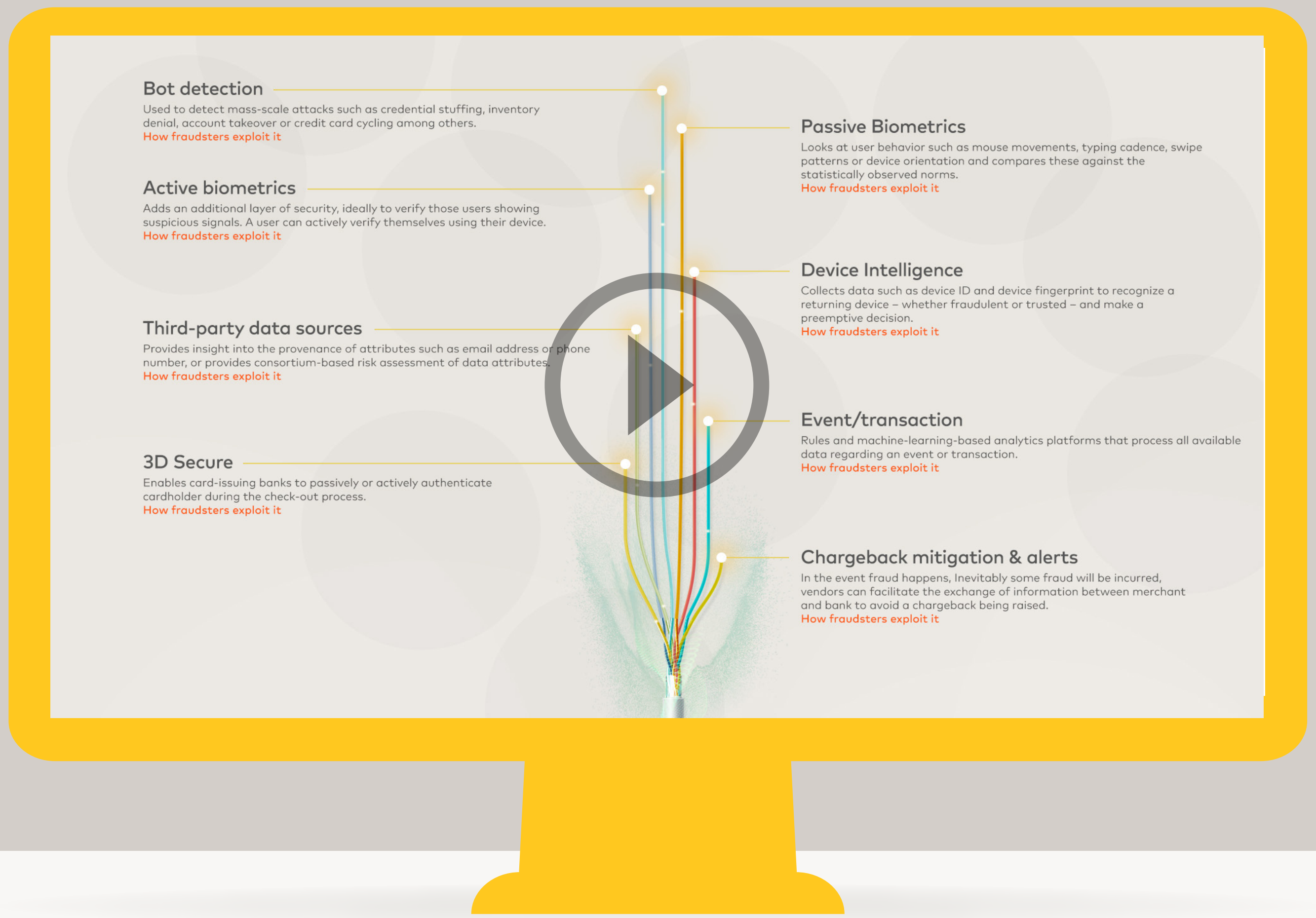
Clearly, current fraud strategies are not only costing issuers and merchants substantial revenues, but consumer loyalty as well: When consumers are mistakenly declined, 24% stop shopping with that retailer and 51% use another card[2].

What is needed today is a multilayered approach to payment security that assesses risk, reduces the need for unnecessary friction, enhances decisioning, and optimizes the consumer experience.

Armed with a coordinated set of AI-based solutions and greater data and insights—what we call Mastercard's Connected Intelligence approach—issuers and merchants can drive a seamless experience that is nearly invisible to the consumer.

[1] U.S. Dept. of Commerce, Quarterly Retail E-commerce Sales YOY Q1 2018, U.S.

[2] Javelin Advisory Services, Addressing the Threat of False Positive Declines, October 2018.



Bot detection

Used to detect mass-scale attacks such as credential stuffing, inventory denial, account takeover or credit card cycling among others.

How fraudsters exploit it

Active biometrics

Adds an additional layer of security, ideally to verify those users showing suspicious signals. A user can actively verify themselves using their device.

How fraudsters exploit it

Third-party data sources

Provides insight into the provenance of attributes such as email address or phone number, or provides consortium-based risk assessment of data attributes.

How fraudsters exploit it

3D Secure

Enables card-issuing banks to passively or actively authenticate cardholder during the check-out process.

How fraudsters exploit it

Passive Biometrics

Looks at user behavior such as mouse movements, typing cadence, swipe patterns or device orientation and compares these against the statistically observed norms.

How fraudsters exploit it

Device Intelligence

Collects data such as device ID and device fingerprint to recognize a returning device – whether fraudulent or trusted – and make a preemptive decision.

How fraudsters exploit it

Event/transaction

Rules and machine-learning-based analytics platforms that process all available data regarding an event or transaction.

How fraudsters exploit it

Chargeback mitigation & alerts

In the event fraud happens, Inevitably some fraud will be incurred, vendors can facilitate the exchange of information between merchant and bank to avoid a chargeback being raised.

How fraudsters exploit it

This approach looks at the entire consumer journey—employing a suite of security solutions that work together and progressively learn from each other at every point of interaction. Fraud detection starts when the consumer journey begins. As the user interacts with their device or account and continues down the purchasing path, through checkout, authentication, authorization, and dispute resolution—each interaction leads to another security layer with more insights and confidence gained at every step all the way to the authorization decision. To help issuers make smarter decisions, Mastercard uses the enormous volume and variety of insights available; physical and behavioral biometrics; device intelligence, location, and spend patterns; and artificial intelligence (AI) and machine learning. Building a fully connected approach to fighting fraud takes time, but a carefully considered strategy to bring it to life can drive lasting impact.

What follows are five steps to help merchants and financial institutions embark on this journey: from evaluating the current internal landscape and getting organizational buy-in, to defining the security layers and authoring rules based on insights along the way.

Step 1

EVALUATING THE POTENTIAL IMPACT TO YOUR ORGANIZATION

Step 2

GETTING ORGANIZATIONAL BUY-IN

Step 3

DEFINING THE IDEAL SECURITY LAYERS, TOOLS, AND INSIGHTS

Step 4

DESIGNING WORKFLOWS, AUTHORING RULES, AND DETERMINING CHALLENGES

Step 5

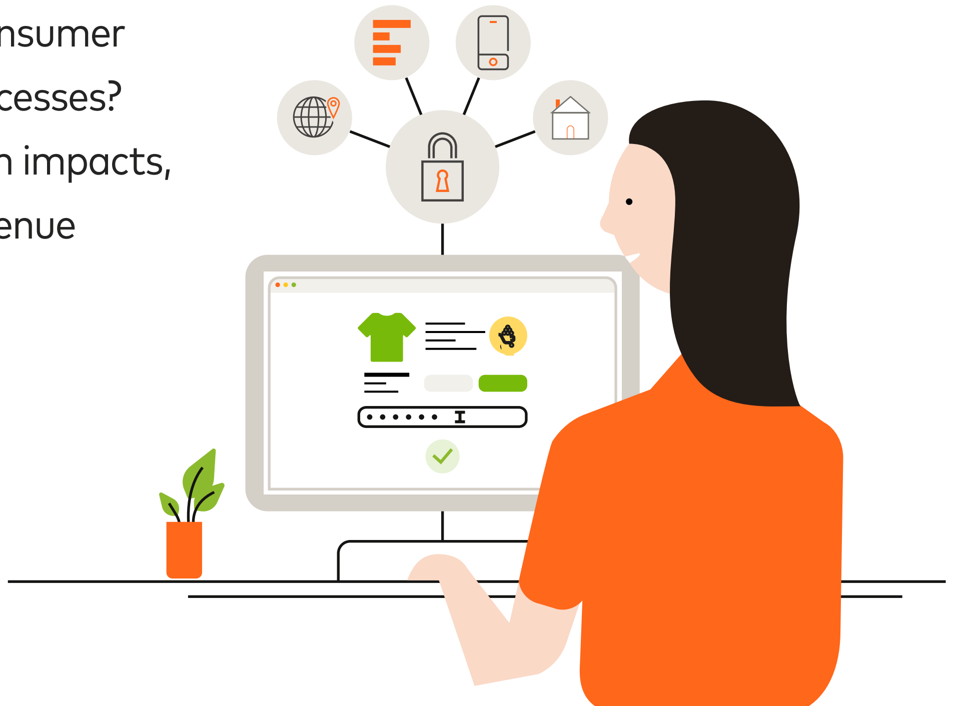
INFUSING INTELLIGENCE INTO THE EQUATION

STEP 1

EVALUATING THE POTENTIAL IMPACT TO YOUR ORGANIZATION

What do you need to bring the Connected Intelligence approach to your organization? To benefit from smarter decisioning throughout the consumer journey, it is imperative to first understand your current state. It all starts with business strategy and objectives. Most likely, you already have some data and insights to begin outlining benchmarks and developing KPIs. The easiest place to start is with revenue targets, fraud losses, and false declines. From there you can start to filter down into specific tactical elements.

From a revenue perspective, naturally, your organization seeks to capture as much of the digital commerce pie as possible—projected to reach $3.3 trillion in the U.S. by 2024[3] —while minimizing losses due to fraud or false declines. To start optimizing the balance of risk versus reward, get a detailed and accurate picture of how fraud is affecting your operations downstream. For example, are increasing e-commerce volumes and changing consumer behaviors placing a strain on current manual fraud monitoring processes? Forecasting your expected losses due to fraud, and its downstream impacts, will help identify how you can contribute to your organization's revenue targets.

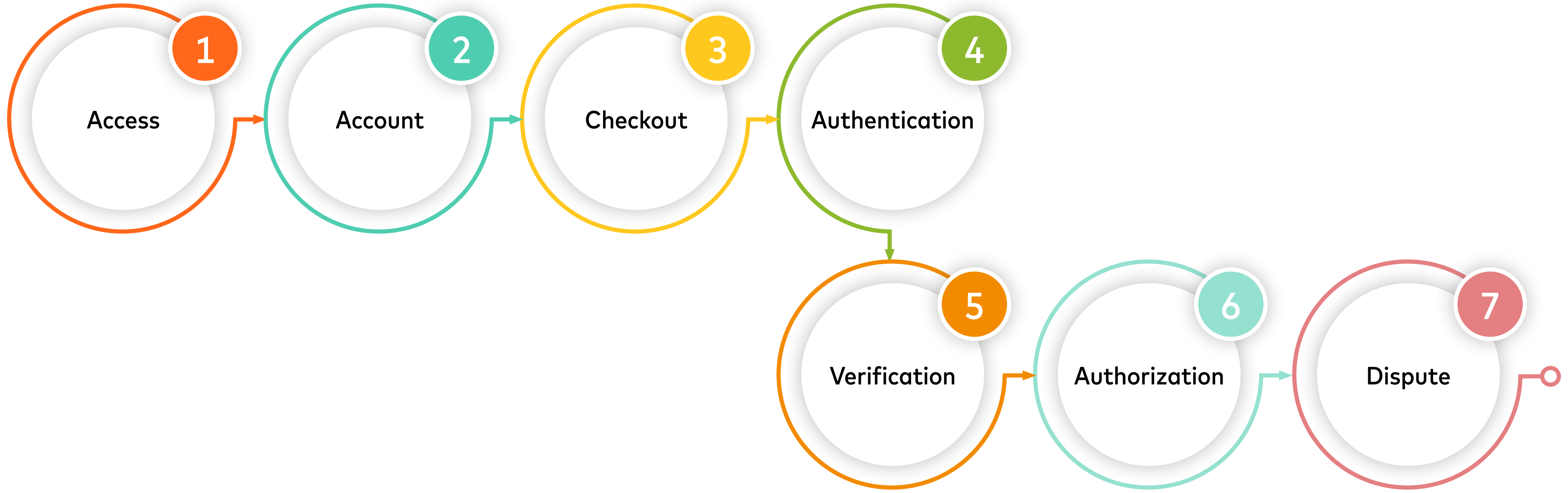


[3] Juniper Research, Digital Commerce Coronavirus Analysis Impact Assessments & Market Forecasts, NAM, April 2020

The Engagement to Decisioning Journey

In order to get granular, consider the multiple touchpoints along the consumer journey where fraud can enter the system—from account creation and account login, to checkout, and even after the transaction, days later.

By mapping out each step and quantifying fraud losses at each point of vulnerability, it becomes clearer where the greatest opportunity for improvement is.



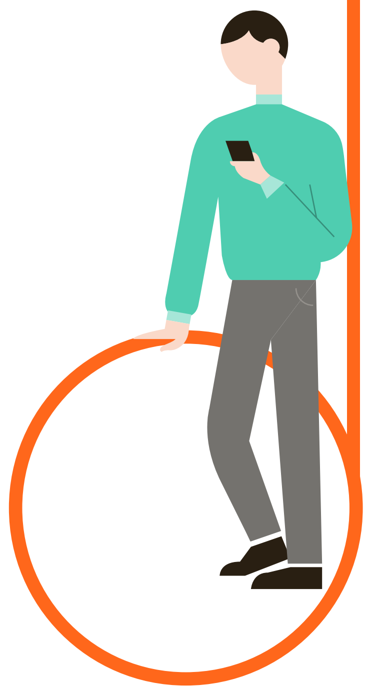
A key insight during this evaluation will come from accurately identifying real vulnerabilities from mere symptoms. For example, a chargeback is an easily identifiable data point, but the chargeback may only be a symptom of a deeper problem—that of online account origination fraud, in which case the account itself is fraudulent. Identifying trends and patterns, such as seasonality associated with specific types of fraud, will also provide insights as to the true source of fraud in the system.

Setting benchmarks and KPIs

After mapping the points of vulnerability across the consumer journey, establish a set of benchmarks and KPIs that ladder up to business objectives.

Benchmarks help identify any changes in activity or behavior after new processes or technology is implemented. Metrics such as login failure rate, abandonment rate, conversion rate, or chargeback rate help identify trends as traffic and fraud evolves.

These benchmarks will then help define the KPIs that fulfill your business objectives, which can take many forms, such as enhancing the consumer experience reducing false declines, lowering chargeback losses, and increasing share-of-wallet and revenue. By tying specific fraud-related KPIs with corporate strategic objectives, you will have an easier time finding funding and support to start moving your fraud numbers in the right direction.



Recommended KPIs

- Average time to checkout
- Average clicks to conversion
- Conversion rate
- Cart abandonment rate
- Percentage of users stepped up
- CNP approval rates
- False positive issuer authorizations
- Fraud BPS on CNP transactions
- Revenue growth
- Loss reduction
- Chargeback rate
- Consumer satisfaction
- Consumer retention

Evaluation Checklist

□ What are your current fraud rates and peak times or seasons?

□ Where along the consumer journey, does your organization experience the most fraud?

□ Are you able to identify the true source of fraud versus a symptom of another gap?

□ What data can you gather from what you believe is your weakest link?

□ How are you currently protecting your users and your digital environment from potential threats?

□ Are you using artificial intelligence, machine learning, or behavioral biometrics?

□ How much time is spent manually monitoring potentially fraudulent behavior?

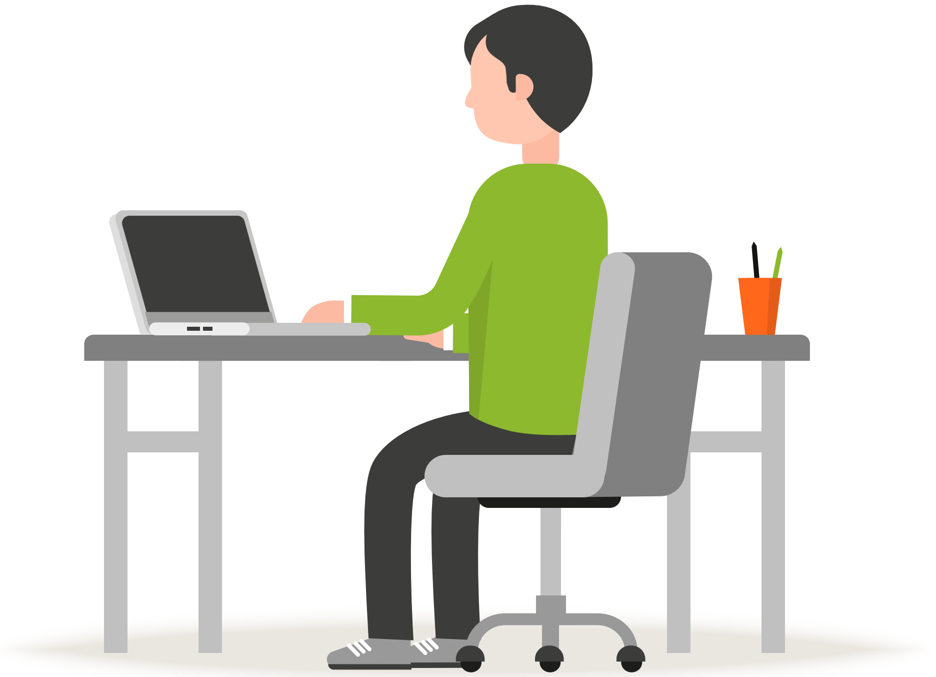
□ What are your projected digital commerce sales?

STEP 2

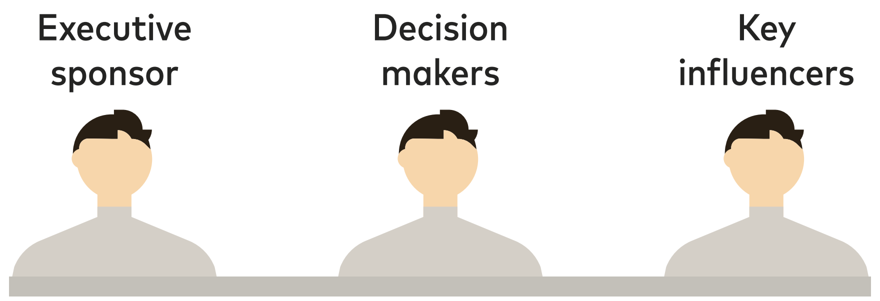
GETTING ORGANIZATIONAL BUY-IN

Now that you have analyzed the fraud and consumer experience gaps in your organization, it is time to get organizational buy-in for a Connected Intelligence approach. Fraud and user experience have often been dealt with by different departments within an organization. But as the consumer journey grows more complex, multifaceted, and multi-device-based, the points of interaction have grown, as have the opportunities to optimize performance.

First, the stakeholders you need to bring on board may vary, depending on your goals. The user experience team may care more about the native app and shopping cart abandonment, while the fraud team may see a reduction in fraud in a specific channel as the most important challenge. Consider your tech stack and who is needed to implement the solutions. Are you able to outline the benefits of this decisioning approach for each stakeholder, perhaps through the business case? How much of a commitment are you requesting from each team member?



Next, seek to ensure alignment with leadership and break down any "insight silos" that may get in the way of collaboration. The heads of technology, digital experience/innovation, fraud, data should share information with each other for a coordinated effort to stop fraud and enhance the customer experience. This could include considerations for security/fraud tools, tactics, techniques and procedures, and perhaps most importantly how the teams and tools would work together. An integral part of ensuring success during this step is to have the full support of your executive sponsor so that decision makers and key influencers remain engaged.



Roll over each stakeholder to learn more

What does your ideal team look like?

The following short list of departments will have a point of view or valuable insights to share and can serve as a starting point to kickstart a conversation on a Connected Intelligence approach, and may serve as decision makers and/or key influencers:

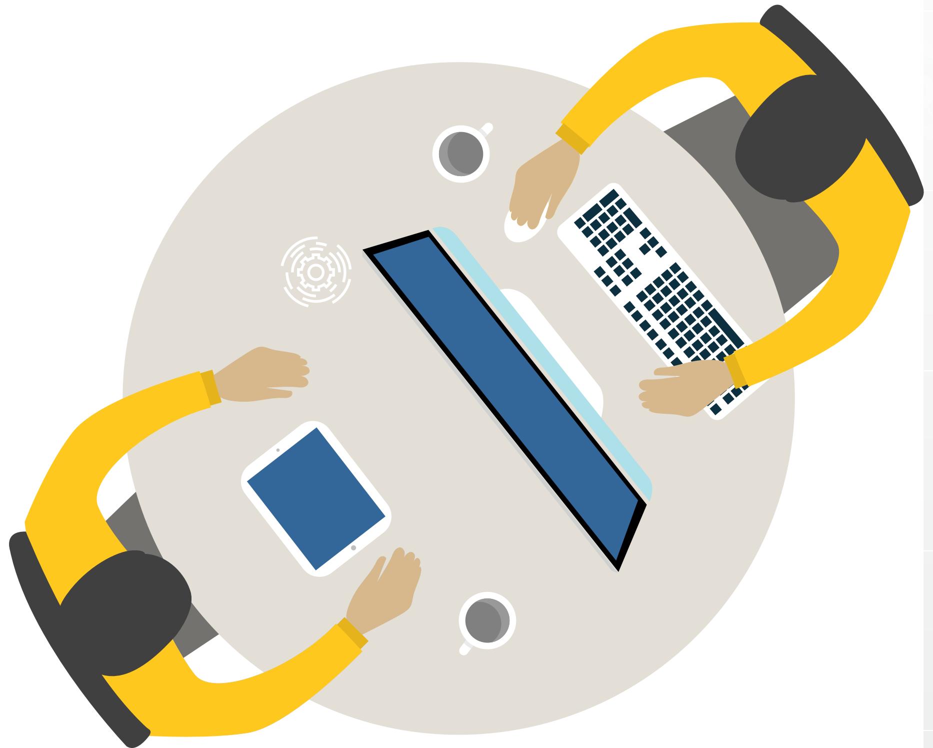
- □ Fraud and/or risk
- □ Fraud strategy
- □ Cyber and info security
- □ Payment strategy
- □ E-commerce experience
- □ User experience
- □ Consumer service
- □ Dispute resolution
- □ Business continuity

STEP 3

DEFINING THE IDEAL SECURITY LAYERS, TOOLS, AND INSIGHTS

Mastercard's model for Connected Intelligence can help your organization identify what's needed for more confident decisioning using the data and insights captured at each point of the consumer journey. Whether you are a financial institution or merchant, monitoring your traffic across a transaction, from start to finish, helps to make better informed decisions on verification and authentication.

For a fully connected approach to succeed, the intelligence gained from each security/fraud prevention layer should inform the subsequent tools along the path, thereby connecting insights for a more confident approval decision.



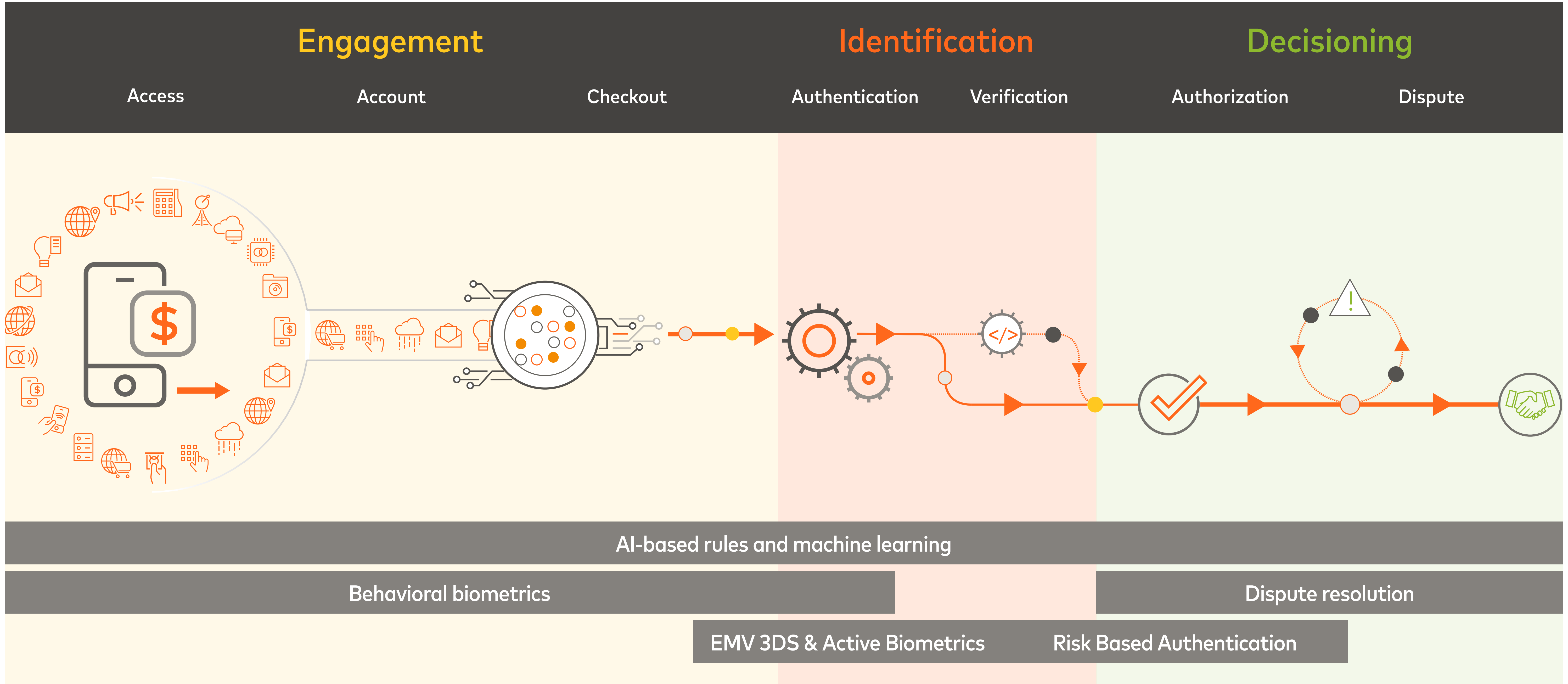
A **MERCHANT** has more control in the early steps in the user journey, where data captured prior to and during checkout can:

- Help recognize a trusted user from a bot attack through behavioral biometrics, enabling your system to mitigate the login or account creation attempt right away
- Identify anomalies and share them with the other tools to prevent fraud at a later stage
- Bypass the needs for static passwords when using the EMV 3-D Secure protocol to harness over 150 data elements to authenticate the user
- Invoke an authentication challenge through methods such as active biometrics to authenticate a user if the data and insights captured don't provide enough confidence for the merchant

An **ISSUER**, on the other hand, can use the insights and data signals from the merchant when making an authorization decision to help them:

- Know if a user has been verified as a good user and not a bad actor based on signals sent from the merchant
- Ingest rich EMV 3-D Secure data from the merchant and use a risk-based authentication tool to make a more confident approval decision
- Increase approval rates based on additional insights from the multiple layers of security in place

Mastercard's Connected Intelligence Approach



Engagement | Identification | Decisioning

Access | Account | Checkout | Authentication | Verification | Authorization | Dispute

AI-based rules and machine learning

Behavioral biometrics

Dispute resolution

EMV 3DS & Active Biometrics

Risk Based Authentication

This approach can also be used for dispute resolution: by sharing insights during the transaction, issuer and merchant can more accurately protect against fraudulent purchases, and even post-purchase friendly fraud.

Today's authentication and authorization decisions can't depend on a single fraud/security tool; rather, different tools along the journey each plays an important role and, as we'll see in the next couple of steps, each can bolster the confidence level of the next.

Checklist of capabilities to consider

□ Behavioral biometrics to verify good users from bad actors

□ EMV 3-D Secure program in place for a more frictionless checkout experience and a more confident issuer approval decision

□ Active biometrics when more data is required, giving consumers a more intuitive, seamless authentication experience

□ Risk-based authentication to make the process of authenticating a user quicker and easier and reduce manual processes

□ A dispute resolution/chargeback process designed for today's digital commerce ecosystem

□ AI and machine learning capabilities that span the customer touchpoints

STEP 4

DESIGNING WORKFLOWS, AUTHORING RULES, AND DETERMINING CHALLENGES

With the right tools identified, you should now be thinking about increasing the risk/reward ratio at each security layer. Every new connection and every new API increases an organization's potential points of vulnerability. Whether it's thwarting an individual fraudster, or a more persistent threat that continuously probes, learns, and evolves, designing a system to meet your needs means having the right rules and workflows in place to make the most of the security tools you have. All rules should be managed by a robust governance program based on your organization's risk tolerance and should establish clearly defined KPIs as discussed in Step 1.

At the highest level, consider the following three pillars of a journey we introduced in Step 3 and what rules govern each pillar: Engagement; Identification and Decisioning.

Optimize Your Engagement Tools

Engagement begins with accurate fraud detection as a user interacts with their device or account. Unique behaviors, such as typing speed, cadence, pressure used on a device, and how often they are accessing the site, are some indicators to help identify the difference.

When implementing rules, the behavior/indicator thresholds can be adjusted based on the organization's comfort level. For example, lower levels at account creation compared to a higher risk event at log in.

Impact of Proper Engagement Tools

- A large global bank was experiencing "constant major account takeover attacks that are bypassing our current defense solution"
- Within the first two weeks of using NuDetect, over half a million fraudulent attempts were blocked that would have otherwise been missed
- 250 million automated attacks were mitigated

Optimize Your Identification Tools

As the user moves past engagement and into identification, it's critical to reduce the amount of assessments and false positives that force good consumers to experience unnecessary friction. Different thresholds and rules will apply to different types of consumers. For example, leveraging the EMV 3-D Secure protocol, an issuer may be able to identify a cardholder based on a combination of data elements—IP address, location, time of day—in which case, the confidence level that this is a good user may be high and the risk score may be low. There may be enough information to offer a frictionless user journey, even bypassing passwords as a result of the risk-based authentication tool deeming it unnecessary. However, if that same user happens to be engaging on a new device or at an unusual time of day, one might consider two-factor authentication to further verify the user. This should take the form of a dynamic form of authentication such as biometrics or one-time passcode (OTP) to build up the user's score to a risk level that the issuer deems acceptable.

Impact of Proper Identification Tools

- A clothing retailer wanted to reduce CNP fraud and increase approvals—specifically on higher-risk cross-border transactions
- By authenticating all CNP transactions with Mastercard Identity Check (3-D Secure), they realized a net fraud rate 20 times lower than their peers, while also increasing sales
- $1.3 million annual fraud savings
- $298 million estimated increase in sales

Optimize Your Decisioning Tools

Finally, using insights gained throughout the journey—from verification all the way to authentication—can help inform authorization strategies leading to smarter decisioning. Whether the insights and data are coming from EMV 3-D Secure, from additional insights passed along by the merchant such as Address Verification Service (AVS) or card validation code 2 (CVC2), or even from behavioral biometrics at the beginning of the consumer journey, issuers have to make a decision.

With risk-based authentication tools, the authorization process is built on a coordinated set of AI-based solutions, which has benefits downstream as well. Not only can good consumers more easily make purchases, but there are efficiencies gained from removing manual fraud rules to more automated ones that can adapt to changing signals. The rules and risk thresholds set up by the issuer will have a large impact on bottom line revenue for issuers and merchants alike.

Impact of Proper Decisioning Tools

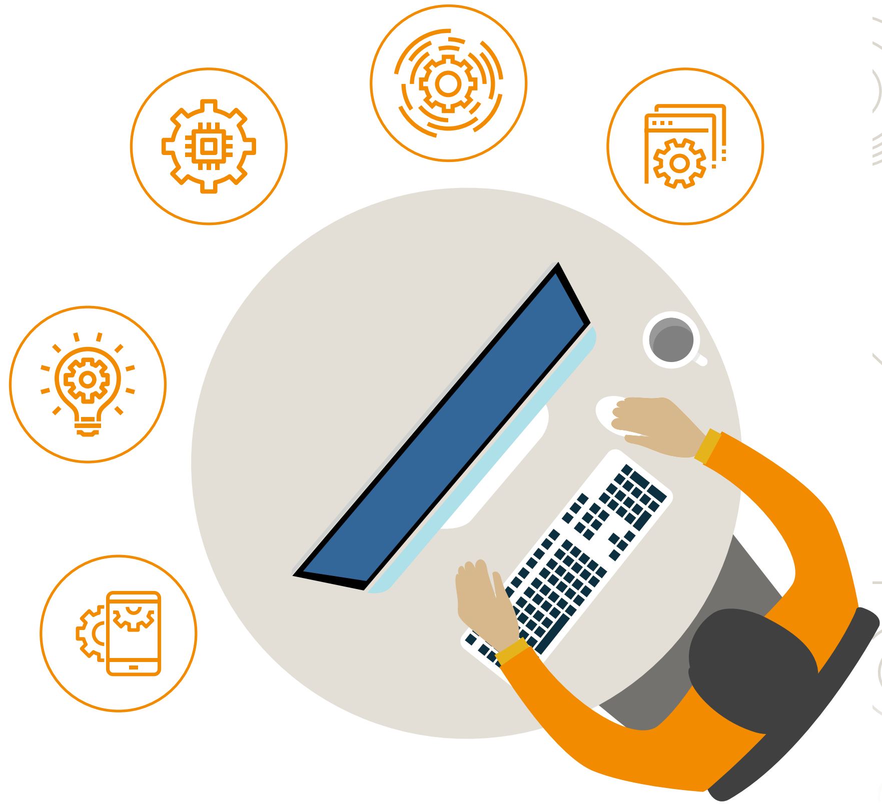
- A top U.S. issuer wanted to reduce chargeback costs, operational expenses, and losses from growing e-commerce fraud
- Using Ethoca's collaboration network, a Mastercard company, over 78,000 chargebacks were mitigated and millions of dollars in fraud were recovered within a 13-month period
- Over $9 million in total chargebacks mitigated

STEP 5

INFUSING INTELLIGENCE INTO THE EQUATION

Upon determining the proper rules and workflows and having enough data available from behavioral and passive biometrics technologies, and protocols like EMV 3-D Secure, you can benefit from a more connected approach.

Unlike static authenticators in wide use today, Mastercard's Connected Intelligence approach leverages machine learning and AI to continuously learn from every interaction and adapt to new and evolving threats from the time a user enters the online environment. This means your organization can be further protected from constantly evolving vulnerabilities, resulting in greater accuracy over time, while providing the consumer a seamless journey.



The value of machine learning and artificial intelligence

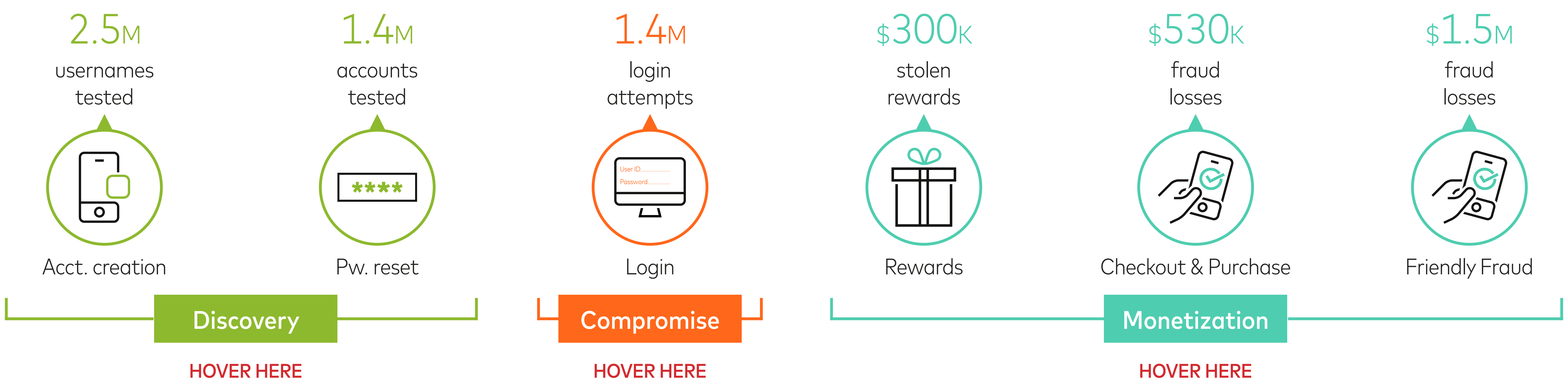
By building AI and machine learning into the full spectrum of a user journey, each step benefits from decisioning models that evolve in response to changing patterns. As data gathered by the different tools feed into the machine learning models, they learn from each event. If there is abnormal traffic volume from a particular device type, the model can flag it and also learn from that anomaly for future decisions. This technology helps you automate complex decisions from each interaction and reduce manual reviews and other manual adjustments.

Where along the consumer journey can AI have the greatest impact?

The addition of machine learning and AI into your fraud prevention strategy can have a dramatic effect on your organization's bottom line. If we bring back our three pillars of the journey, we can see the impact at each pillar.

By infusing intelligence and leveraging the insights gained along the way from one step to the next, here's an example of the impact that Mastercard's Connected Intelligence approach can have on the organization:

Engagement	Identification	Decisioning
Monitor behavioral interactions of the consumer and account accessing the ecosystem	Review customer's payment credentials, verify user identity, and tokenize credentials	Score fraud risk using enhanced AI models and rules, manage disputes and complete order seamlessly



2.5M usernames tested — Acct. creation

1.4M accounts tested — Pw. reset

Discovery

HOVER HERE

1.4M login attempts — Login

Compromise

HOVER HERE

$300K stolen rewards — Rewards

$530K fraud losses — Checkout & Purchase

$1.5M fraud losses — Friendly Fraud

Monetization

HOVER HERE

Assess the intelligence of your fraud prevention strategy

- □ Do you have a model that can adapt to sudden changes in traffic or behaviors?
- □ Does your model leverage broad, anonymized data sets to constantly evolve?
- □ What parameters or factors can your model learn from?
    - □ Sudden change of login failure rate
    - □ Sudden change in expected browser use
    - □ Sudden increase of traffic from unexpected location
- □ Do your fraud prevention tools share insights with each other?
- □ Are your models using static data or dynamic data to assess risk levels?

Seamless & Secure:
Mastercard's Connected Intelligence Approach

Digital commerce is the new normal, and connected consumers don't distinguish between physical and digital channels. They expect the same seamless, secure experience across the consumer journey. But the preponderantly static and manual risk management tools employed by financial institutions and merchants don't have the necessary agility to combat the increasingly sophisticated tactics of fraudsters. The result: issuers and merchants are losing much more revenue by mistakenly declining legitimate purchases than they lose to actual CNP fraud.

By using these steps as a guide, and leveraging Mastercard's Connected Intelligence approach, issuers and merchants can reduce fraud and improve the user experience. By connecting the dots between all the points of interaction along the consumer journey and leveraging the data and insights gleaned from each point, you gain a more holistic view of the consumer to make more informed decisions. The benefits of Mastercard's approach go straight to your bottom line:

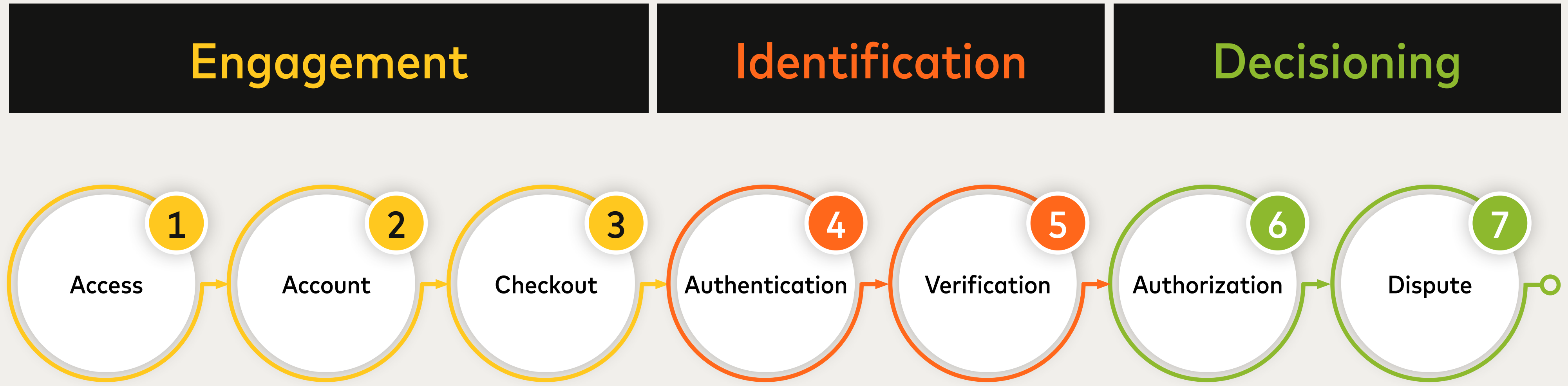
Enhance the consumer experience by delivering a more consistent, seamless, secure shopping experience across devices, while reducing false declines

Grow business and revenue by approving more genuine transactions and reducing vulnerabilities

Reduce operational expenses by lowering chargebacks, and other service costs and by reducing manual fraud reviews

Invest for the future by leveraging advanced technologies like biometrics, risk-based authentication, and AI

Mastercard's Connected Intelligence Approach



For more information about Mastercard's Connected Intelligence approach, visit **mastercard.com/authentication**

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.