Targeted card fraud protection: How to fortify existing defenses

PLAYBOOK • AUGUST 2026

Contents

Fraud decisioning in an evolving threat landscape

Fraud decisioning exists because fraud is persistent, adaptive and unavoidable. Even in highly secured payment channels, attempted fraud never fully disappears — it evolves. As controls improve, fraudsters probe transaction flows, test responses and iterate until they identify gaps that can be exploited at scale.

This reality makes fraud prevention a continuous decisioning challenge, not a one-time implementation effort. Controls that perform well today can degrade over time if left unchanged while attackers actively search for moments of weakness created by new behaviors, new channels or operational constraints.

Decisioning is not just stopping fraud

Fraud decisioning is often mischaracterized as a simple approve-or-decline exercise. Effective **decisioning is optimizing outcomes across competing objectives**, not maximizing a single metric in isolation.

If eliminating fraud were the only goal, the solution would be trivial: decline every transaction. While that approach would prevent losses, it would also interrupt legitimate activity, undermine trust and significantly diminish long-term value for both issuers and cardholders.

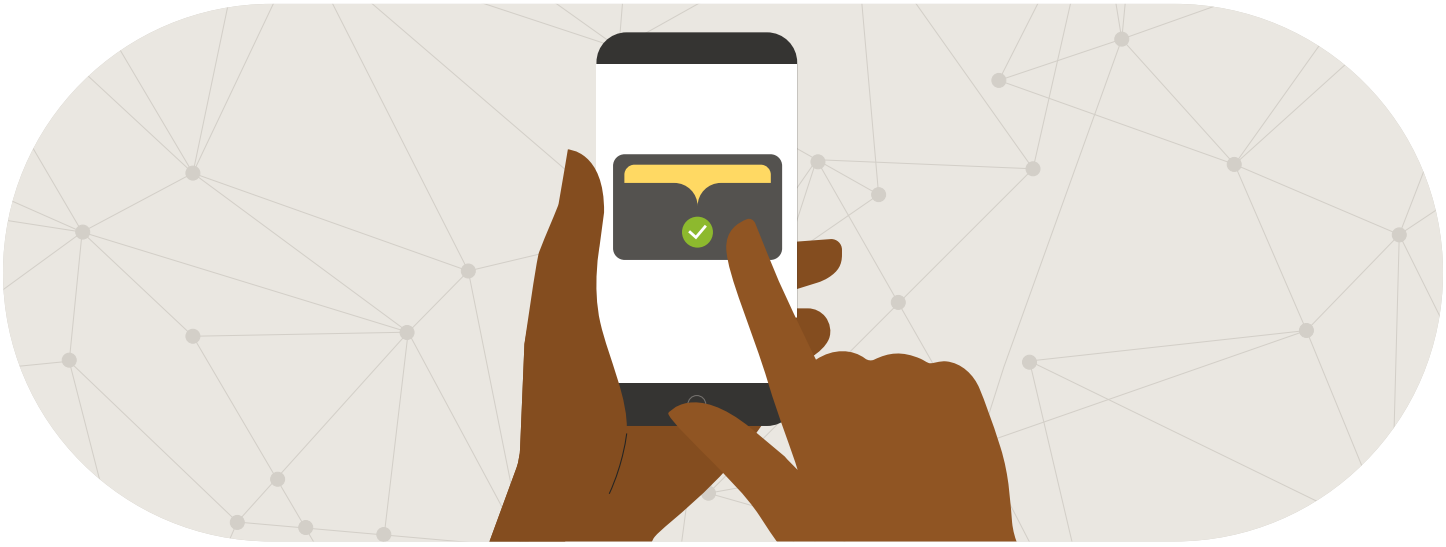
From a cardholder's perspective, the expectation for an ideal experience is far more nuanced.

- Legitimate transactions are approved seamlessly.
- Exposure to fraud feels minimal or invisible.
- Suspicious activity is identified quickly.
- Notifications are timely and clear.
- Remediation actions — such as reimbursement or reissuance — are effective without being disruptive.

At the same time, issuers must operate within real-world constraints. Fraud decisioning must balance, simultaneously:

- managing fraud risk exposure
- preserving a smooth customer experience
- maintaining operational efficiency across alerts, reviews and recovery processes

Because these objectives can conflict with one another, the goal of fraud decisioning is not perfection. It is **measured balance** — making informed trade-offs that minimize harm while maximizing overall outcomes.



Why fraud performance is measured in trade-offs

Because fraud outcomes are **inherently imperfect**, performance is rarely measured in absolutes. Most fraud programs instead rely on relative metrics that quantify **trade-offs** across risk, customer experience and operational impact.

Common examples include:

- fraud basis points, which place fraud losses in context relative to transaction volume
- false positives, which quantify customer friction resulting from unnecessary declines

More advanced fraud teams extend beyond these surface-level indicators by evaluating **how effectively fraud is identified and contained relative to total exposure**, while keeping customer disruption and operational workload in check. This broader lens shifts the focus from simply asking whether fraud was stopped to understanding **how efficiently decisioning performs across the portfolio**.

In this context, rule authors often reference detection efficiency measures such as:

- **value detection rate (VDR)**, which reflects the proportion of total fraud value successfully identified or mitigated
- **transaction detection rate (TDR)**, which measures the share of fraudulent transactions detected relative to all attempted fraud

Together, these measures help teams assess the **quality of decisioning**, balancing loss prevention against customer experience and operational cost, rather than optimizing any single metric in isolation.

How Mastercard Rule Cartridges support fraud decisioning

Mastercard Rule Cartridges are designed to support this continuous optimization challenge. Designed to work directly with the Decision Intelligence product, Mastercard Rule Cartridges supplement fraud mitigation strategies and enhance decisioning. They are **not intended to replace issuer strategies or eliminate fraud in isolation**.

Instead, they provide **structured, network-informed decisioning layers** that help issuers respond to evolving fraud patterns while maintaining balance across risk, customer experience and operational outcomes.

Mastercard Rule Cartridges — Overview

What are Mastercard Rule Cartridges?

Rule Cartridges are packaged, on-behalf decisioning rule sets developed and maintained by Mastercard to address fraud patterns observed across the broader payments ecosystem. They provide baseline fraud protection by leveraging consortium level intelligence derived from issuer-reported fraud activity.

Rather than focusing on issuer-specific configurations or a single fraud vector, Rule Cartridges reflect **shared ecosystem behavior** — patterns that impact multiple issuers operating in similar environments. This enables issuers to benefit from network-level insight that **protects them against fraud patterns observed across peers, including scenarios that may not yet be visible within their own portfolios**.

How they work

Rule Cartridges are designed to deliver broad, stable coverage while minimizing unnecessary friction. At a high level, they operate as follows:

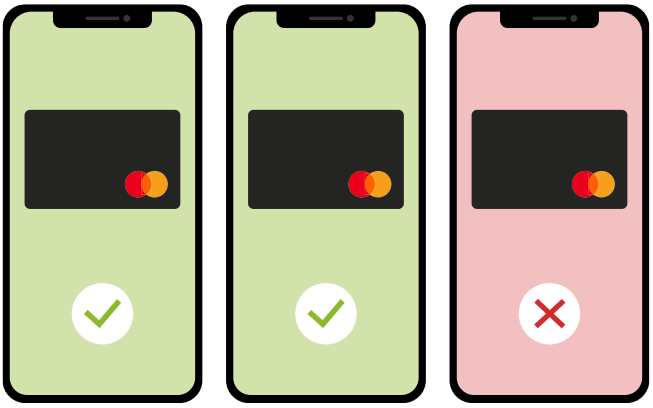
Ecosystem-informed baseline protection
The rule set targets fraud patterns that are actively affecting issuers within similar markets or operating environments. It is based on aggregated ecosystem insight — rather than isolated issuer history.

Regular refresh cadence
Rule Cartridges are updated on a recurring basis (commonly quarterly) to incorporate emerging fraud patterns, recalibrate thresholds and remain aligned with upstream data and model changes.

Balanced, multi-vector design
Each Rule Cartridge contains multiple rules addressing different fraud behaviors, intentionally tuned to balance fraud detection, approval rates and operational impact.

Operationally simple adoption
Issuers enroll in a packaged rule set rather than individual rules. Once enabled, the Rule Cartridge runs on behalf of the issuer, who selects whether transactions result in alerts or declines.

DI Pro score modification capability
Decision Intelligence (DI) Pro score modification is a Rule Cartridges capability that allows Mastercard-authored rules to override or adjust the DI Pro score on a transaction when an issuer-specified rule condition is met. This enables rules to act directly on the DI Pro score (999) outcome, not just to generate alerts or reason codes.



The types of Mastercard Rule Cartridges that we offer

Mastercard offers multiple different types of Rule Cartridges designed to meet specific requirements and use cases for issuers. The next sections will go over all the different types of Rule Cartridges we currently offer.

- **Market level:** Dynamic, multi-layered, precision-crafted rule sets designed to address multiple regional fraud vectors. These are refreshed on a quarterly cadence.
- **Targeted**: Rule Cartridges purpose-built to target a specific fraud pain point or vector. By focusing on a narrow fraud use case, these Rule Cartridges can apply more aggressive rules, often accepting higher false positives in exchange for deeper coverage of that vector.

Market-level Rule Cartridges — Summary

Market-level Rule Cartridges represent the baseline layer of the Rule Cartridges portfolio. They are designed to deliver broad, ecosystem-informed decision-making that is aligned with how fraud manifests across markets, providing consistent protection grounded in shared market behavior.

What market-level Rule Cartridges represent

- **Regional baseline protection** informed by fraud patterns observed across issuers operating within the same market or environment
- A proactive decisioning layer aligned to peer behavior, including **fraud patterns an issuer may not yet have encountered directly**
- Broad, multi-vector coverage intentionally tuned to balance **fraud detection, customer experience and operational impact**

What market-level Rule Cartridges are not designed to do

- They **do not replace** issuer fraud systems or internal decisioning strategies.
- They **do not provide issuer-specific customization**; the rule set is built to reflect shared market behavior.
- They **are not intended for narrow, single-issue optimization**, instead prioritizing **balanced stability and broad coverage across fraud types**.

A use case example of how the Rule Cartridges work

- The issuer requests enrollment of specific **account ranges** into a Mastercard Rule Cartridge. No additional technical implementation is required. Protection begins as soon as enrollment is active.
- An authorization request is sent through the Mastercard network.
- The transaction matches one or more fraud mitigation rules within the Rule Cartridges.
- Based on the issuer's selected action mode:
  - **Alert Mode**: The transaction is tagged with an **RA (Rule Alert)** in **DE 48.75.02**.
  - **Decline Mode**: The transaction is declined by Mastercard, and an **RD (Rule Decline)** is sent in **DE 48.75.02**.
- Even when enrolled in **Alert Mode**, the issuer retains final decision authority.

For example, the issuer may:

- read the **RA reason code** in their fraud system
- automatically create a case and validate with the cardholder
- decline the transaction using their own decisioning rules

As a result, the issuer receives **immediate protection against fraud patterns** they may not have written rules for themselves.

Please reach out to your local sales representative to find out what the most up-to-date market-level Rule Cartridges offerings in your area are.

Targeted Rule Cartridges

Targeted Rule Cartridges provide **focused segmentation** where issuers request additional decisioning depth for a specific fraud pattern or transaction context. They are designed to build on baseline coverage by concentrating on defined areas of risk, while remaining consistent with the broader Rule Cartridges decisioning framework.

How Targeted Rule Cartridges help

- Deeper decisioning in priority areas by mapping each **targeted Rule Cartridge** to a specific, well-defined issuer risk or control need.
- Serve as an **entry point** for issuers not enrolled in market-level Rule Cartridges.
- Work best in environments where there is **sufficient transaction volume** in the targeted segment to support meaningful outcomes.
- For issuers already enrolled in market-level Rule Cartridges, targeted Rule Cartridges are designed to **add depth without re-covering the same ground**. Incremental value is created by narrowing the decisioning lens to a specific fraud pattern or transaction context, allowing for **more focused tuning** and outcomes while **preserving the stability of the baseline rule set**. This approach avoids duplicating existing coverage and instead **layers additional precision** where issuers see concentrated risk or emerging pressure, ensuring improvements are additive rather than redundant.

Targeted Rule Cartridge	Markets available
Authentication	U.S., LAC
Tokenized transaction	U.S.
Money transfer	U.S.
Crypto transaction	U.S., LAC
Suspicious merchant	U.S.

01

Authentication Rule Cartridge

This Rule Cartridge is not an **authentication or ACS/3DS control** and does not introduce friction, step-ups or challenges for the cardholder. It operates entirely in the **authorization rail**, using authentication context as an input to support better decisioning once a transaction reaches authorization.

The intent is not to influence how authentication is performed, but to recognize that successful authentication does not eliminate downstream risk.

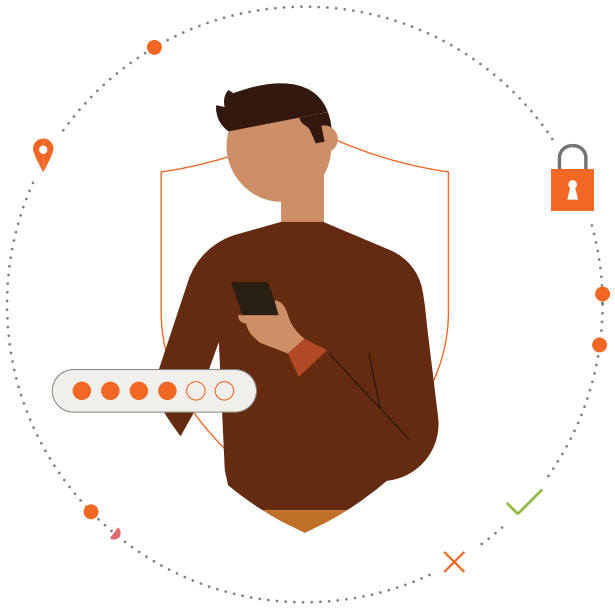
Why this coverage is needed

A meaningful share of fraud is observed on transactions that have already passed through authentication successfully. These situations often involve scenarios such as **social-engineering scams, identity compromise, account takeover** or other forms of authorized misuse where the cardholder is deceived or credentials are abused. In these cases, authentication may function exactly as designed, yet fraud still materializes later in the flow.

This creates a gap that cannot be addressed through authentication controls alone and requires **authorization-side decisioning** to manage exposure.

What the Rule Cartridge is designed to do

This Rule Cartridge is **not intended to address the root causes** of post-authentication fraud. Its purpose is to **limit financial impact** by strengthening authorization decisions when risk remains after authentication has been completed. By segmenting transactions based on how they progressed through authentication — such as frictionless, challenged or data only — and **applying authorization-side decisioning informed by Mastercard network insights and data inputs**, the rule set enables more precise outcomes without adding customer friction or disrupting baseline protections.



02

Tokenized transaction Rule Cartridge

This Rule Cartridge is designed for **authorization-side decisioning in tokenized payment flows**, with a **focus on fraud patterns that occur within tokenized transactions themselves**. It evaluates how fraud manifests once tokens are in use, rather than how or why a token was created.

Tokenization is treated strictly as **transaction context**, not as a security guarantee. The Rule Cartridge **does not introduce friction** or alter how tokenization or provisioning processes operate upstream.

Why this coverage is needed

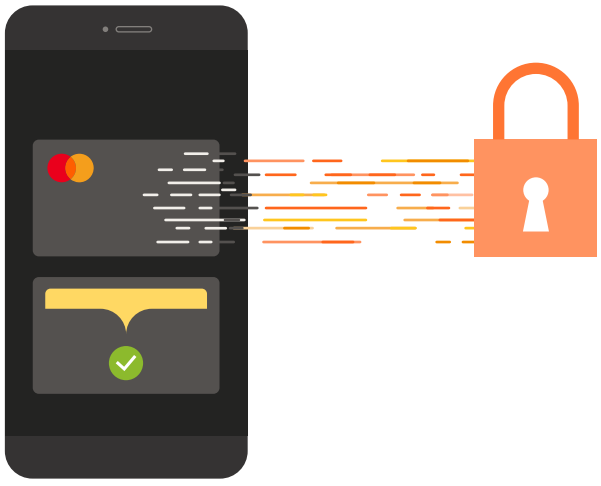
While tokenization improves security by reducing the exposure of primary account data, **fraud continues to occur within tokenized transactions**, often exhibiting **distinct behavioral patterns** compared to non-tokenized flows. As tokenized payments scale across both card-present and card-not-present environments, issuers increasingly observe fraud that reflects **how tokens are used in practice** — including abnormal reuse, replay behavior or misuse within specific digital contexts — rather than failures in authorization controls alone.

In some cases, **gaps or limitations in provisioning-stage controls** can also contribute to downstream risk, allowing **compromised credentials** or deceptive enrollment scenarios to result in valid tokens being created and later misused. Once those tokens are active, fraud manifests **within the tokenized transaction stream itself**, where baseline decisioning may not fully differentiate tokenized and non-tokenized behavior. This creates a need for **additional segmentation** that treats tokenized activity as a distinct transaction context, enabling more precise authorization-side decisioning without extending friction or broadening controls unnecessarily.

What the Rule Cartridge is designed to do

This Rule Cartridge is **not intended to address the root causes** of fraud in tokenized ecosystems. Instead, it focuses on **reducing financial impact** by strengthening **authorization decisions** when fraud is observed within tokenized payment flows.

By **identifying tokenized transactions through network indicators** and applying authorization-side decisioning informed by Mastercard network insights and data inputs, the rule set enables more precise outcomes in this segment. This allows issuers to contain losses in tokenized channels without disrupting baseline protections or overgeneralizing controls across the broader portfolio.



03

Money transfer Rule Cartridge

This Rule Cartridge is designed for **authorization-side decisioning within money transfer transactions**, where transaction intent and risk characteristics differ materially from general purchase activity. It focuses on fraud patterns observed in money transfer use cases, rather than broader consumer spending behavior.

It is not a **velocity management** or **customer communication tool**, and it does not attempt to control how money transfer services operate, such as **Mastercard Send™ issuer transaction controls**. The Rule Cartridge does not assess customer intent or legitimacy directly; money transfer activity is treated solely as transaction context at authorization.

Why this coverage is needed

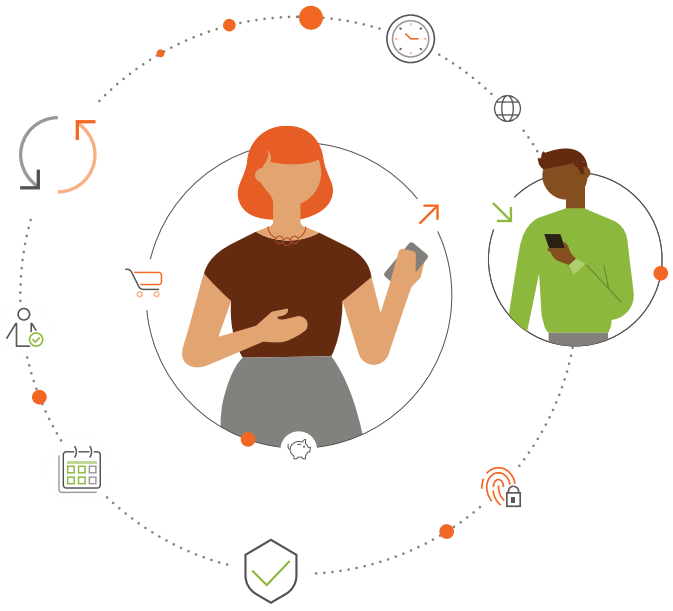
Money transfer transactions are disproportionately impacted by **social-engineering scenarios**, where cardholders are manipulated into initiating transfers that appear legitimate at the transaction level. These cases often involve scams, coercion or deception and frequently pass traditional authorization checks because the cardholder is actively participating.

As a result, fraud in this segment often concentrates within specific merchant categories, transaction patterns or transfer behaviors that are **not always well addressed by broader baseline controls**. Issuers may observe elevated losses only after patterns become established, creating a gap where **targeted authorization-side decisioning** is needed to manage exposure.

What the Rule Cartridge is designed to do

This Rule Cartridge is designed to **apply focused authorization-side controls where money transfer activity exhibits elevated risk**, particularly in scenarios influenced by social engineering. Rather than broadly tightening controls across the portfolio, it enables issuers to **concentrate on decisioning within the money transfer segment**, where losses tend to cluster.

By leveraging **segment-specific indicators and Mastercard network insights**, the rule set helps issuers contain fraud tied to money transfer misuse without attempting to diagnose scam mechanics or disrupt legitimate transfer activity outside the affected segment.



04

Crypto transaction Rule Cartridge

This Rule Cartridge is designed for **fraud prevention at authorization for card-based crypto purchases**, where cards are used to fund or buy crypto through on-ramp merchants and platforms. It focuses specifically on **fraud patterns associated with crypto purchase transactions**, not on broader crypto activity.

It is **not an AML, sanctions or financial-crime monitoring solution**, and it does not perform transaction tracing, source-of-funds analysis or regulatory checks. The Rule Cartridge does not evaluate crypto platforms, wallets or assets, and it does not establish issuer policy on crypto usage. Crypto purchases are treated strictly as a **fraud-relevant purchase context at authorization**.

Why this coverage is needed

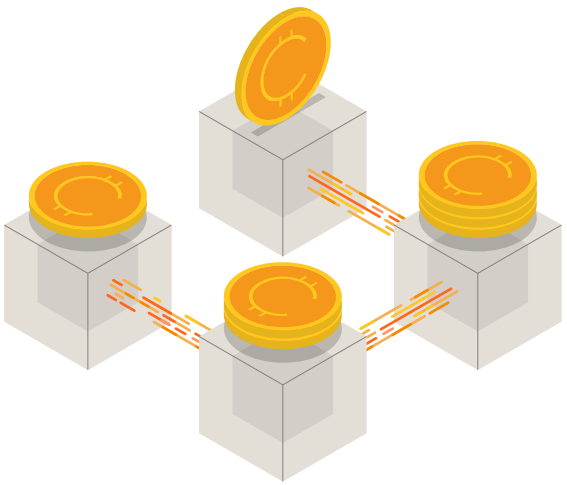
Crypto purchase transactions are frequently involved in **fraud scenarios driven by social engineering, scams or credential compromise**, where cardholders are manipulated into initiating purchases that appear legitimate at the point of sale. In these cases, the transaction often looks like an ordinary purchase, even though the underlying risk is elevated.

For many issuers, crypto purchases represent **a concentrated source of fraud losses relative to their overall transaction volume**. Losses can escalate quickly before patterns are visible using issuer-only data, while broad restrictions on crypto merchants risk disrupting legitimate customers. This creates a gap where **purchase-specific fraud risk exists**, but baseline decisioning does not sufficiently distinguish crypto on-ramp transactions from everyday commerce.

What the Rule Cartridge is designed to do

This Rule Cartridge is designed to **detect and contain fraud when it manifests in crypto purchase transactions**, applying authorization-side controls informed by **Mastercard network fraud patterns and purchase-level indicators** associated with crypto on-ramps.

The rule set helps issuers **apply tighter, purchase-specific decisioning** where fraud risk is elevated. The focus is on **loss containment within crypto purchases**, allowing issuers to respond proportionally without extending restrictive controls across unrelated spend.



05

Suspicious merchant Rule Cartridge

This Rule Cartridge is designed for **authorization-side decisioning informed by merchant behavior**, focusing on fraud patterns where **merchant activity itself may be a meaningful driver of risk**. It evaluates how transactions behave when they are associated with merchants exhibiting unusual or high-risk signals across the ecosystem.

This is not an acquiring solution and does not provide merchant monitoring, investigation or enforcement capabilities, such as **Mastercard Merchant Monitoring, Mastercard Merchant Risk Predict or the Questionable Merchant Audit Program (QMAP)**. The Rule Cartridge does not initiate merchant reviews, take action against merchants, or replace acquirer or network compliance processes. Merchant behavior is used strictly as an authorization-time decisioning context for issuers.

Why this coverage is needed

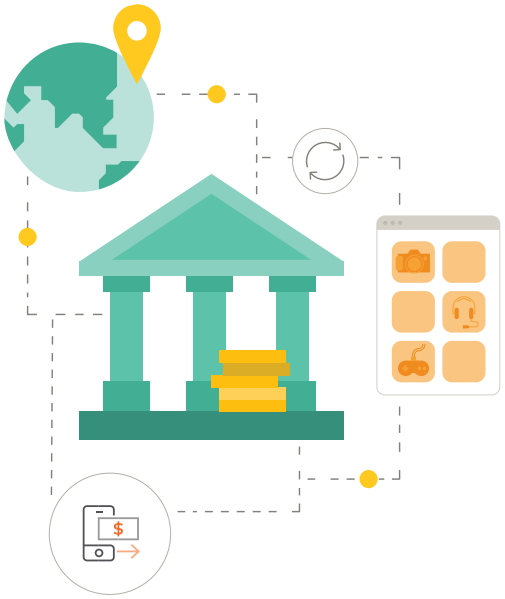
In certain fraud scenarios, losses are driven less by individual cardholder behavior and more by **merchant-related risk**, such as abnormal transaction patterns, rapid changes in merchant activity or ecosystem signals that suggest elevated exposure. These situations often span multiple issuers, making it difficult for any single issuer to recognize the pattern early using issuer-only data.

Because issuers typically have **limited visibility into cross-ecosystem merchant behavior**, exposure can accumulate before the risk becomes apparent. This creates a gap where merchant-level signals are highly relevant to decisioning but not easily operationalized within standard authorization strategies.

What the Rule Cartridge is designed to do

This Rule Cartridge enables issuers to **identify and act on merchant-driven risk at authorization**, where patterns of merchant behavior observed across the **Mastercard network** materially elevate potential exposure. Rather than applying broad controls, it supports **selective intervention** when transactions intersect with merchants exhibiting suspicious or high-risk activity.

The focus is on **concentrating decisioning where risk clusters**, using **Mastercard ecosystem merchant signals** to inform authorization outcomes without changing cardholder behavior or expanding controls beyond the affected segment. This allows issuers to limit losses tied to merchant behavior while maintaining stability across the rest of the portfolio.



Conclusion

As new card fraud tactics and vulnerabilities abound, the need for issuers to use global insights and intelligence to develop efficient and effective fraud-prevention rules is clear.

Using data effectively is crucial to staying ahead of opportunistic fraudsters, ensuring that prevention measures are targeted and adaptable for future challenges.

Issuers have the opportunity to strengthen defenses strategically and precisely, implementing efficient rules for robust and scalable protection.