



REPORT
SEPTEMBER 2026

A lifecycle view of payment fraud

Why 99% of cards don't follow a linear fraud cycle:
What Mastercard sees instead.



Payment fraud is no longer a sequence; it's a signal lifecycle

“

Fraud rarely announces itself.

For most fraud practitioners, it starts quietly — an isolated signal, a single alert or a compromised card tied to a merchant. On its own, it may not seem urgent. But somewhere else in the ecosystem, that same card may already be tested, listed for sale or have been used fraudulently. The challenge is detecting fraud while also understanding how these signals connect and when they matter most.

Traditionally, fraud has been viewed as occurring in a clean sequence: cards are compromised, then tested and finally used for criminal gain. This model suggests a clear path and predictable progression. In reality, fraud does not behave so neatly.

Signals appear out of order. Multiple actors interact with the same card data simultaneously. A compromised card can move directly to fraud, bypassing testing or marketplace exposure altogether—or surface in multiple environments at once. Fraud practitioners are not dealing with a single, linear chain, but a fragmented system of signals that must be interpreted in context.

This creates a fundamental problem.

Which signals should fraud practitioners act on, and how fast?

To answer this, Mastercard analyzed compromised card activity across digital skimming, card testing, marketplace exposure and reported fraud. Instead of forcing these signals into a fixed sequence, the analysis examined how they appear, overlap and evolve in real-world environments.

What emerges is a different way of understanding fraud risk—not as a sequence of events, but as a signal lifecycle.

Key findings

For fraud practitioners, one of the biggest challenges is knowing which signals matter, and when to act on them. Mastercard analysis of Primary Account Numbers (PANs) associated with observed digital skimming activity shows that compromised card risk is better understood as a signal lifecycle than as a fixed fraud sequence. Digital skimming, card testing, marketplace exposure, and reported fraud each provide a different level of confidence, urgency, and operational value for fraud teams.

- The full sequence of digital skimming, card testing, marketplace exposure, and fraud was rarely observed. This reflects the limits of observable signals, fraudster behavior and marketplace visibility.
- Signal type is a strong indicator of how soon fraud is expected on a card. When digital skimming was observed before fraud, the median time to fraud was 96 days. When card testing was observed before fraud, the median time to fraud was less than one day, meaning fraud occurred the same day of observed card testing.
- Issuers can use these signals to prioritize PAN-level monitoring, authorization controls, case escalation and selective reissue. Acquirers can use the same signals to prioritize merchant investigation, remediation and recurring compromise review.

Compromised card signal lifecycle: digital skimming, card testing, marketplace exposure and fraud outcomes

Digital skimming is the theft of payment card data from compromised e-commerce merchants, often through malicious scripts, compromised checkout pages, vulnerable site plugins or third-party services. Digital skimming represents one of the most common methods criminals use to steal payment card data. For issuers, digital skimming is a PAN compromise signal, and for acquirers, it is a merchant compromise signal. For both, it can be an early indicator of downstream risk.

Mastercard analyzed PANs associated with observed digital skimming activity to understand what other Mastercard-visible fraud signals appeared for those same PANs. The analysis included card testing, card marketplace exposure and reported fraud.

This analysis should not be read as a complete fraud kill chain. Digital skimming was used to identify the PAN sample, and it was not assumed to be the first observed event for every PAN. The order of signals was determined by observed timestamps so other signals may have appeared before or after the skimming observation.

The resulting view is a compromised card signal lifecycle. The lifecycle is useful because each signal has a different meaning.

Signal	Meaning	Operational value
Digital skimming	PAN associated with compromised digital merchant environment	• Compromise signal • Early risk awareness
Card testing	PAN observed in activity consistent with fraudulent or malicious card validation	• Urgency signal • Rapid escalation
Marketplace exposure	PAN or card data observed in monetization environment	• Confidence signal • Severity increase
Reported fraud	Confirmed downstream fraud activity	• Outcome signal • Control tuning and impact measurement

“

The value for fraud practitioners at banks is not in proving every step occurred. It is in understanding what each signal says, how strong it is, how close it may be to fraud and which response is appropriate.



Observable compromised-card lifecycle in Mastercard data

When these signals are observed in real-world environments, they rarely follow a clean progression. Instead, they appear in fragmented and uneven patterns.

“
Missing signals should not be interpreted as absence of risk.

Mastercard observed four primary signal types for PANs within the identified sample: digital skimming, card testing, marketplace exposure and reported fraud.

These should be understood as observable signal categories rather than required sequential stages. A PAN may show one signal, several signals, or all signals and missing signals should not be interpreted as absence of risk. They may reflect activity that did not occur, activity that occurred outside Mastercard-visible sources or limitations in marketplace visibility.

It's also important to note that a card may be exposed through multiple sources, which can create irregular or seemingly contradictory activity patterns. As a result, different fraudsters may possess the same compromised card data simultaneously, with one engaging in testing or fraudulent use while another attempts to monetize the card by listing it on a marketplace.

The most common observed paths included:

- Digital skimming to fraud
- Digital skimming to card testing to fraud

The full path of digital skimming to card testing to marketplace exposure to fraud was rarely observed with only 0.1% of all cards moving through all four observable signals.

Even when one signal is observed, progression to additional signals is far from guaranteed—but it does increase risk meaningfully with each observed signal.

Observed conversion rates were:

Signal relationship	Observed conversion
One observed signal to two observed signal	11.6%
Two observed signals to three observed signals	12.5%
Three observed signals to four observed signals	8.9%

The table above summarizes progression rates between observed signals. Because these signals do not always occur in the same sequence, the reported percentages capture the occurrence of observing additional signals, rather than progression through a fixed set of stages. Overall, 11.6% of the total sample moved from the first observed signal to a second observed signal. Of those with a second observed signal, 12.5% went on to experience a third observed signal, while 8.9% of those with a third observed signal subsequently experienced a fourth observed signal.

0.1%

of all cards move through all four observable signals

FINDINGS

Time to intervene within the lifecycle

Understanding how signals appear is only part of the picture—timing ultimately determines their operational value. Timing differs sharply by signal, which was a vital takeaway throughout this research.

Signal relationship	Median days
Digital skimming to card testing	15
Card testing to marketplace exposure	35
Marketplace exposure to fraud	19

Additional timing observations:

Signal relationship	Median days
Digital skimming to fraud	96
Card testing to fraud	<1

The timing between digital skimming and fraud indicates a potential intervention window when skimming is observed before fraud. A median of 96 days allows time for monitoring, risk scoring, customer segmentation and targeted intervention.

Card testing has different implications. The median time from card testing to fraud was less than one day. This signal is extremely close to fraud where slow manual review may not materially reduce fraud losses. Card testing should be treated as a high-urgency signal and connected to faster controls where possible.

This urgency is reflected in observed historical outcomes. Mastercard Threat Intelligence (MTI) provides actionable intelligence on cards it identifies with card testing activity. Based on internal Mastercard analysis, in the first half of 2026, cards protected by MTI experienced approximately 70% lower subsequent fraud reporting rates than cards where testing activity was approved by issuing banks.

These findings also revealed critical insights in understanding how to respond to certain signals. It showed that digital skimming and card testing should not be handled with the same operational posture. Digital skimming supports earlier risk awareness and prioritization where card testing supports much more immediate escalation.

Signal strength and appropriate use

Each signal should be weighted differently. Digital skimming identifies compromise. It is useful for early monitoring and prioritization, but it does not mean fraud is certain. For issuers, it can support PAN-level monitoring and risk scoring. For acquirers, it can support merchant investigation and remediation.

Card testing indicates active validation that the PAN could go on to be used for fraudulent purposes. It is a stronger urgency signal, because fraud may follow quickly. For issuers, it should influence near-real-time authorization controls, step-up logic, fraud review, and selective reissue decisions. For acquirers, it can increase urgency when tied back to exposed PANs from a compromised merchant environment.

“Card testing should be treated as a high-urgency signal and connected to faster controls where possible.”

Marketplace exposure adds monetization context. It can increase confidence that compromised card data has entered criminal commerce. However, lack of marketplace exposure should not be treated as evidence that the PAN is safe. Marketplace visibility is partial by nature. The addition of new and previously unknown marketplaces, tactics to evade detection by legitimate organizations and the usage of alternate channels (such as social media platforms) make it difficult to maintain full visibility into marketplaces.

Reported fraud confirms downstream impact. It should be used to tune future controls, assess which earlier signals were present and measure where intervention may have been possible.

19

Median days between marketplace exposure to fraud

<1

Median day from card testing to fraud



Responding to fraud signals

Mastercard research supports a move away from static detection models towards a dynamic, lifecycle-based approach to fraud risk management. Fraud signals do not follow a clean sequence, and each signal develops into fraud on a unique timeline.



For fraud practitioners at issuing banks:

- **Act on exposure signals earlier:** Digital skimming should be treated as an early indicator of potential compromise, enabling enhanced monitoring and risk-based assessment before fraud occurs. Relying solely on the presence of additional signals may delay intervention and reduce the window to mitigate losses.
- **Escalate validation signals immediately:** Card testing should be treated as a near-term fraud indicator, requiring rapid authorization controls, step-up authentication or selective reissue rather than delayed manual review.
- **Use marketplace exposure to increase severity:** Marketplace exposure should increase confidence and urgency, supporting reissue decisions, PAN prioritization and clustering analysis—but its absence should not be used to dismiss exposure or testing signals.
- **Use outcomes to refine decisioning:** Confirmed fraud should be used to assess which signals were present beforehand, helping issuers identify missed intervention windows and improve risk models over time.



For fraud practitioners managing merchant risk:

- **Identify and investigate compromised merchants:** Digital skimming should trigger investigation of merchant environments, including checkout pages, scripts, and third-party integrations, to identify and address sources of exposure.
- **Prioritize remediation based on signal escalation:** Merchants linked to multiple signals—such as card testing or fraud—should be prioritized, as overlapping signals indicate a higher likelihood of active exploitation.
- **Use downstream fraud to strengthen enforcement:** Fraud outcomes should be linked back to merchant environments, supporting stronger remediation actions, escalation and ongoing monitoring of high-risk entities.



For both:

- **Do not rely on a complete lifecycle view:** Fraud signals are often fragmented, and waiting for a full sequence of events can delay action until risk has already materialized.
- **Align response to timing and signal strength:** Early-stage signals enable monitoring and prioritization, while validation signals require immediate action, making timing the critical factor in response strategy.
- **Interpret signals based on their role in the lifecycle:** Exposure, validation, monetization and confirmed fraud each convey different levels of urgency and should be acted on accordingly rather than treated uniformly.

In a fragmented signal environment, the advantage does not come from seeing every step of the fraud lifecycle—it comes from recognizing what each signal means, how urgent it is and acting before it's too late.

A signal-led approach to fraud detection

Mastercard analysis of PANs associated with digital skimming shows that compromised card risk is better understood through a signal lifecycle than a fixed fraud chain. Digital skimming, card testing, marketplace exposure and reported fraud each provide different types of risk information.

Digital skimming identifies compromises. Card testing indicates active validation and is much closer to fraud. Marketplace exposure adds monetization context and confidence. Reported fraud confirms downstream impact and should be used to improve earlier controls.

The most important operational finding is timing. When digital skimming preceded fraud, the median time to fraud was 96 days. When card testing preceded fraud, the median time to fraud was less than one day. This supports different response

models: digital skimming for monitoring and prioritization, card testing for rapid escalation.

For fraud practitioners at issuing banks, the lifecycle supports earlier PAN-level risk management, more targeted authorization controls, and selective reissue strategies. For fraud practitioners assessing the merchant risk, it supports merchant investigation, remediation prioritization, and stronger linkage between merchant compromise and downstream payment risk.

The value of the lifecycle is not that every PAN follows the same sequence. The value is that each signal helps fraud teams decide what they know, how urgent the risk is and what action is proportionate.

How Mastercard supports lifecycle-based fraud detection

The findings in this report highlight the importance of understanding fraud risk as a lifecycle of signals rather than a fixed sequence of events. Fraud often begins with a cyber incident, and more and more, cyberattacks are red flags for potential fraud. Identifying and acting on these signals earlier can help organizations take action to stop losses before they escalate.

However, translating this understanding into action requires consistent visibility across the payments ecosystem and the ability to identify, connect and prioritize signals in near real time.

Built on Mastercard's unique network visibility and global threat expertise, [Mastercard Threat Intelligence](#) gives payment fraud and risk practitioners a curated view of emerging cyber threats across the payment ecosystem. It delivers targeted intelligence by collecting, analyzing and sharing actionable information through Mastercard Connect®, enabling teams to stay ahead of fraud.

By expanding visibility into evolving payment threats, Mastercard Threat Intelligence enables organizations to:

- ✓ Identify early indicators of compromise, including digital skimming and emerging fraud schemes.
- ✓ Detect and action high-risk activity, such as card testing, that may signal imminent fraud.
- ✓ Gain insight into vulnerabilities across payment software, merchant environments and domain activity.
- ✓ Strengthen collaboration across fraud, risk, compliance and cybersecurity teams by understanding the latest fraud trends.

These capabilities allow fraud practitioners to proactively prevent criminal activity, reduce cyber risk and strengthen their response maturity—supporting a more proactive, lifecycle-based approach to fraud detection and mitigation.



About Mastercard

Mastercard is a global technology company in the payments industry. Our mission is to connect and power an inclusive, digital economy that benefits everyone, everywhere by making transactions secure simple, smart and accessible. Using secure data and networks, partnerships and passion, our innovations and solutions help individuals, financial institutions, governments and businesses realize their greatest potential. With connections across more than 210 countries and territories, we are building a sustainable world that unlocks priceless possibilities for all.

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.

©2026 Mastercard. Mastercard is a registered trademark, and the circles design is a trademark, of Mastercard International Incorporated.

