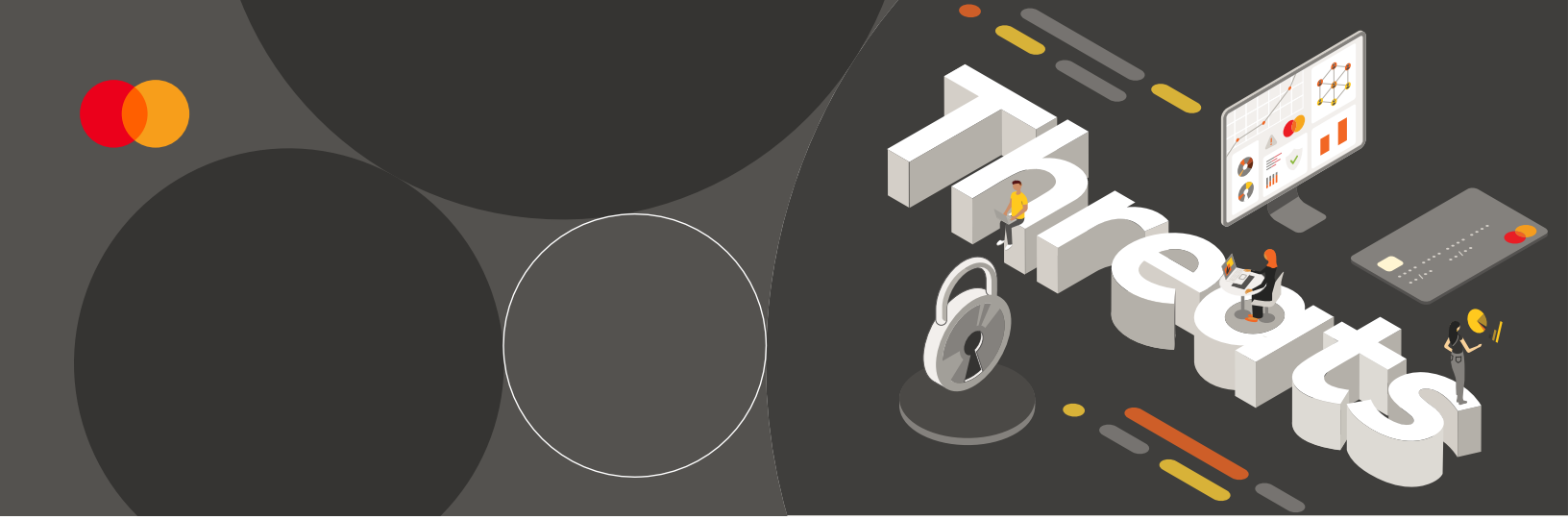


Reduce the impact of payment fraud with Mastercard Threat Intelligence

DATASHEET ● 2026

Mastercard Threat Intelligence gives fraud and risk practitioners a curated, real-time view of cyber threats impacting the payment ecosystem.

Combining Mastercard's global threat expertise with unique payment ecosystem visibility, it delivers actionable intelligence through the Mastercard Connect®, Mastercard Developer Zone APIs, and Fraud Rule Manager, enabling organizations to integrate real-time intelligence into their existing workflows and authorization decisioning.

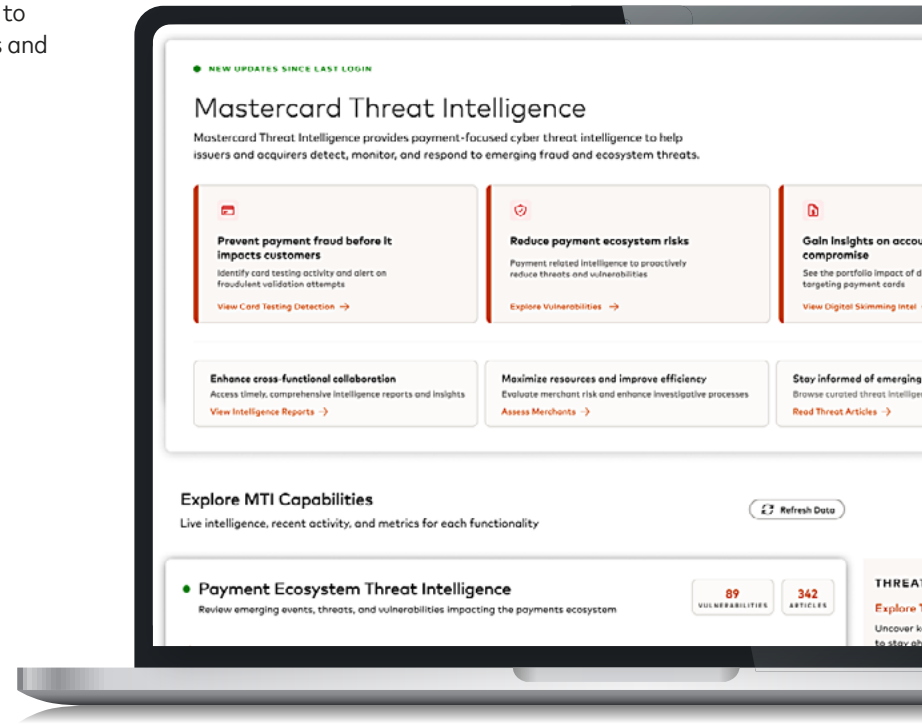
By helping organizations identify compromised cards, card testing activity, risky merchants, and emerging fraud schemes earlier, Mastercard Threat Intelligence enables faster investigations, more effective risk prioritization, reduced fraud losses, and stronger protection for cardholders.

>1 day

Median time from card testing to fraud[1]

77%

of global business leaders reported an increase in cyber-enabled fraud and phishing overall[2]



1. Mastercard. A Lifecycle View of Payment Fraud, 2026.
2. World Economic Forum. Global Cybersecurity Outlook 2026.

Defend against emerging payment threats with Mastercard Threat Intelligence

Key functionalities

Card Testing

Prevent fraud with precision using real-time alerts that flexibly block card testing attempts before criminals can verify card validity.

Criminals use stolen or computer-generated card numbers to test whether they are active, often as the first step in larger fraud schemes. Mastercard helps disrupt this activity by identifying and either declining or alerting on suspected card testing transactions in real time, based on issuer preferences. Card testing signals can also be operationalized within existing fraud workflows, helping issuers prioritize investigations, strengthen controls, and take proactive action to prevent additional fraud. As an early indicator of broader cyber-fraud risk, these signals can help uncover emerging threats before they escalate.

Digital Skimming Intelligence

Understand the impact of digital skimming malware on card holders and efforts that Mastercard has taken to limit exposure.

Digital skimming attacks can expose payment card data long before fraud is detected. Mastercard works with industry partners to identify and disrupt skimming malware while providing quantitative intelligence on affected domains, portfolio exposure, transaction volume, and potential fraud losses. By connecting cyber threat activity to fraud risk, organizations can make faster, more informed decisions and strengthen coordination across fraud and security teams.

Payment Ecosystem Threat Intelligence

Stay informed and responsive to fast-moving payment threats with curated, weekly intelligence built for fraud teams.

Receive tailored updates that surface relevant payment ecosystem risks, such as phishing campaigns, mobile wallet fraud and high-risk e-commerce vulnerabilities. Designed for fraud analysts, this curated feed delivers actionable intelligence and exclusive insights, Fraud teams can respond faster, coordinate with internal cybersecurity teams and stay aligned on emerging risks without needing deep technical expertise.

Payment Intelligence Reports

Empower teams with monthly strategic, expert-led reports and recommendations.

In-depth reports combine Mastercard's data with insights from beyond its network, offering a comprehensive view of activity across the payment ecosystem and deep fraud subject matter expertise. Reports highlight the most pressing fraud trends and risks, with actionable guidance that can be used across the enterprise. Fraud practitioners get access to executive-ready materials, including anonymized case studies, best practices and solution recommendations, to confidently report on threats and support cross-functional alignment.

Merchant Threat Intelligence

Evaluate merchant risk with cyber threat signals beyond transaction data.

Payment fraud and risk practitioners gain targeted threat intelligence to investigate merchant domains. Teams can strengthen fraud investigations by searching for threats and assessing real-time cyber-based signals. As a result, teams get clearer visibility into merchant-level risk, enabling faster, more confident investigations and earlier identification of potential fraud exposure.

Watch how Mastercard Threat Intelligence helps organizations identify payment threats earlier.

Actionable, curated, real-time intelligence built for payments teams

Overcome siloes to fortify your defenses

Mastercard Threat Intelligence bridges gaps between fraud and cyber operations — creating a more connected and resilient response.

Achieve proactive, real-time fraud prevention

Powered by ongoing threat insights and automation, Mastercard Threat Intelligence alerts or acts on behalf of organizations so you can stay ahead of evolving threats.

Act with precision, powered by Mastercard's insights

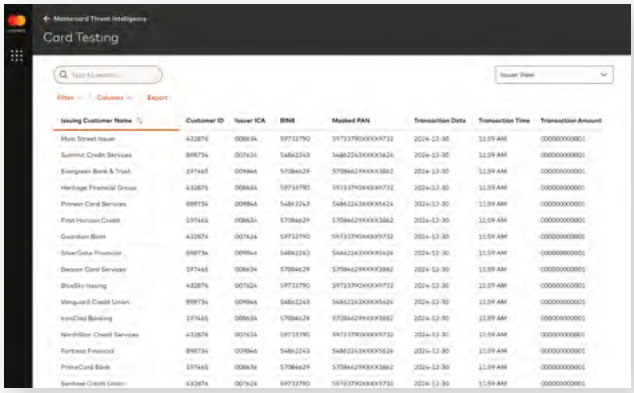
Get clarity on threat responses with intelligence built on Mastercard's global network data, unique visibility and decades of payments fraud expertise.

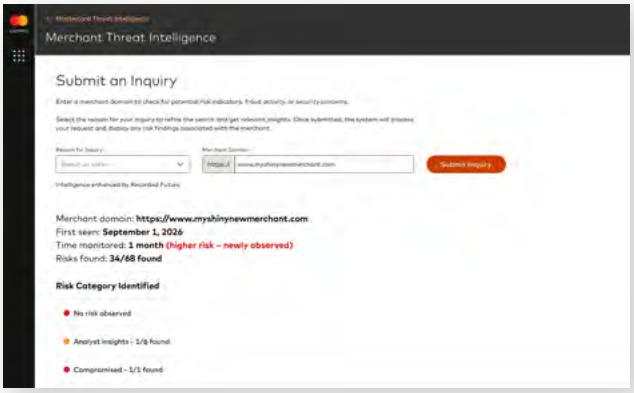
Extend your team without expanding it

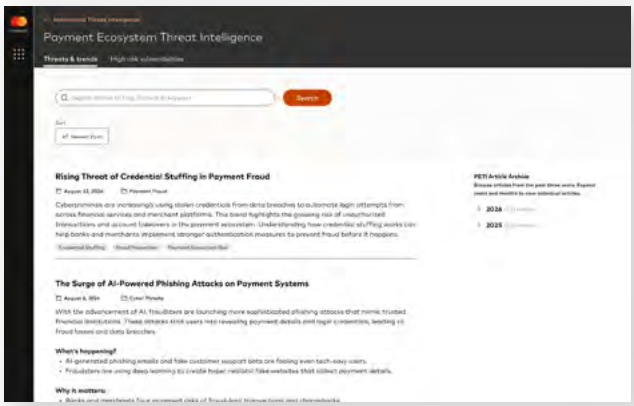
Scale your team with automation and expert insights, empowering faster responses with existing resources.

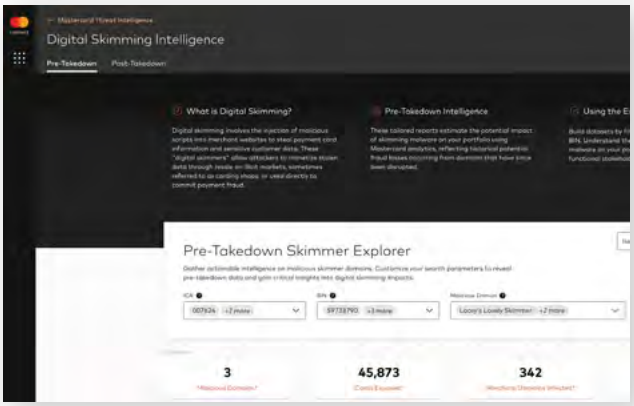
Easy access through Mastercard Connect or API

Mastercard Threat Intelligence is accessible through Mastercard Connect®, with API data feeds available via Mastercard Developer Zone, enabling organizations to integrate intelligence directly into existing fraud, cyber, and risk workflows.









The data displayed in this screenshot is entirely fictitious and is provided solely for illustrative purposes.
Any resemblance to real persons, organizations, or actual data is purely coincidental.

To learn more visit mastercard.com or reach out to threat.intelligence@mastercard.com