



# Reduce the impact of payment fraud with Mastercard Threat Intelligence

ISSUER DATASHEET ● SEPTEMBER 2025

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

Built on Mastercard's global threat expertise and unique network visibility, it delivers intelligence by collecting, analyzing and sharing actionable information through Mastercard Connect® — so organizations can stay ahead of sophisticated fraud and increase their threat response maturity.

By providing ecosystem-wide visibility into evolving payment threats, Mastercard Threat Intelligence allows organizations to rapidly triage incidents such as card testing activity and emerging fraud schemes. It provides situational awareness to detect criminal tactics — including phishing, fraudulent websites and other cardholder-targeted threats — and delivers clear, actionable insights that distill complex threat data into focused intelligence. Teams can respond faster, reduce fraud impact and protect cardholders.

## 57%

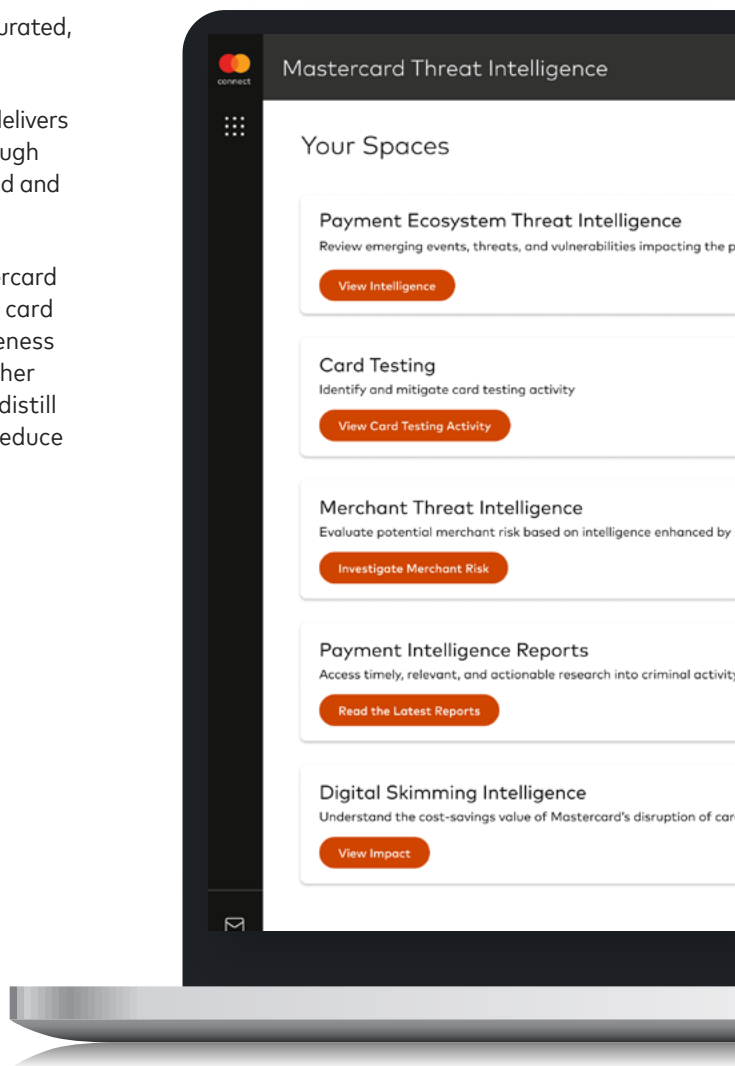
of global fraud executives are notified of cyber breaches only after fraud losses begin<sup>1</sup>

## 59%

of cybersecurity leaders are critically understaffed in threat intelligence areas<sup>2</sup>

1. Datos Cyber Fraud Integration Survey, August 2025.

2. ISACA. State of cybersecurity, 2023 survey report, 2023.



# Defend against emerging payment threats with Mastercard Threat Intelligence

## Key functionalities

### Card Testing

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

Criminals use stolen or computer-generated cards to test for validity, often as the first step in high-impact fraud schemes. Mastercard breaks this fraud lifecycle by identifying testing transactions in real time, declining on behalf of organizations before threats escalate. Card testing identified by Mastercard Threat Intelligence is linked to fraud rates nearly 10x greater than the network average, meaning even a few approvals can lead to significant losses.

### Digital Skimming Intelligence

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

Digital skimming malware is a top driver of card compromise, but organizations often lack visibility into its impact. Mastercard works to disrupt malware and provides quantitative intelligence from domain takedowns. This visibility bridges the gap between fraud and cyber functions and strengthens collaboration.

### 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 reported by their cardholders and assessing real-time cyber-based signals.

### Payment Ecosystem Threat Intelligence

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

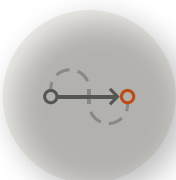
Receive tailored updates that surface relevant payment ecosystem risks, such as phishing campaigns, mobile wallet fraud and high-risk e-commerce vulnerabilities. Designed for fraud analysts and non-cyber specialists, this curated feed delivers actionable intelligence and exclusive insights. Fraud teams 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.

## Actionable, curated 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®

Mastercard Threat Intelligence is provisioned through your existing Mastercard Connect® account — no additional setup required.

Mastercard Threat Intelligence

Card Testing

Search: Test to vulnerability

Filter: All Columns: Export

Testing Customer Name	Customer ID	Issuer ICA	BRN	Masked PAN	Transaction Date	Transaction Time	Transaction Amount
Blue Street Bank	432876	000636	5973790	5973790XXXXX7732	2024-12-30	11:59 AM	0.000000000000000000
Summit Credit Services	898736	001626	54862263	54862263XXXXX0426	2024-12-30	11:59 AM	0.000000000000000000
Evergreen Bank & Trust	577465	009964	5786429	5786429XXXXX3862	2024-12-30	11:59 AM	0.000000000000000000
Heritage Financial Group	432876	000636	5973790	5973790XXXXX7732	2024-12-30	11:59 AM	0.000000000000000000
Power Card Services	898736	009964	54862263	54862263XXXXX0426	2024-12-30	11:59 AM	0.000000000000000000
First Horizon Credit	577465	000636	5786429	5786429XXXXX3862	2024-12-30	11:59 AM	0.000000000000000000
Guardian Bank	432876	001626	5973790	5973790XXXXX7732	2024-12-30	11:59 AM	0.000000000000000000
GreenGate Financial	898736	009964	54862263	54862263XXXXX0426	2024-12-30	11:59 AM	0.000000000000000000
Beacon Card Services	577465	000636	5786429	5786429XXXXX3862	2024-12-30	11:59 AM	0.000000000000000000
BlueDay Insuring	432876	001626	5973790	5973790XXXXX7732	2024-12-30	11:59 AM	0.000000000000000000
Vanguard Credit Union	898736	009964	54862263	54862263XXXXX0426	2024-12-30	11:59 AM	0.000000000000000000
FirstNet Banking	577465	000636	5786429	5786429XXXXX3862	2024-12-30	11:59 AM	0.000000000000000000
NorthStar Credit Services	432876	001626	5973790	5973790XXXXX7732	2024-12-30	11:59 AM	0.000000000000000000
Fortress Financial	898736	009964	54862263	54862263XXXXX0426	2024-12-30	11:59 AM	0.000000000000000000
PrimeCard Bank	577465	000636	5786429	5786429XXXXX3862	2024-12-30	11:59 AM	0.000000000000000000
Summit Credit Union	432876	001626	5973790	5973790XXXXX7732	2024-12-30	11:59 AM	0.000000000000000000

Mastercard Threat Intelligence

Merchant Threat Intelligence

Submit an Inquiry

Enter a merchant domain to check for potential risk indicators, fraud activity, or security concerns.

Select the reason for your inquiry to refine the search and get relevant insights. Once submitted, the system will process your request and display any risk findings associated with the merchant.

Reason for inquiry:  Merchant Domain:

Search on domain:  Submit Inquiry

Intelligence enhanced for Blockchain Future

Merchant domain: <https://www.myshinynewmerchant.com>

First seen: November 30, 2024

Time monitored: 1 month (higher risk - newly observed)

Risks found: 34/68 found

Risk Category Identified

- No risk observed
- No risk observed
- Analyst insights: 1/6 found

Mastercard Threat Intelligence

Payment Ecosystem Threat Intelligence

Threats & Trends High risk vulnerabilities

Search: Test to vulnerability

CVE ID	Risk Score	Lifecycle Phase	Date of Lifecycle Phase	Affected Products & Versions	Assessment
CVE-2024-00000	99	Exploited	14-Feb-2025	Adobe Commerce and 17 more	Exploited in the Wild by Malware
CVE-2024-00000	99	Exploited	12-Feb-2025	WordPress and 12 more	Historically Exploited in the Wild by Malware
CVE-2024-00000	99	Exploited	08-Feb-2025	Adobe Commerce and 17 more	Historically Exploited in the Wild by Malware
CVE-2024-00000	99	Exploited	08-Feb-2025	Adobe Commerce and 17 more	Exploited in the Wild by Malware
CVE-2024-00000	99	Exploited	04-Feb-2025	WordPress and 12 more	Exploited in the Wild by Malware
CVE-2024-00000	99	Exploited	26-Feb-2025	Adobe Commerce and 17 more	Historically Exploited in the Wild by Malware
CVE-2024-00000	99	Exploited	02-Feb-2025	WordPress and 12 more	Exploited in the Wild by Malware
CVE-2024-00000	99	Exploited	29-Jan-2025	WordPress and 12 more	Historically Exploited in the Wild by Malware
CVE-2024-00000	99	Exploited	27-Jan-2025	Adobe Commerce and 17 more	Exploited in the Wild by Malware
CVE-2024-00000	99	Exploited	23-Jan-2025	WordPress and 12 more	Historically Exploited in the Wild by Malware

CVE-2021-32790

Affected Products & Versions

- WooCommerce 3.9.0 Beta 2 for WordPress
- WooCommerce 3.9.0 Release Candidate 1 for WordPress
- WooCommerce 3.9.0 for WordPress
- WooCommerce 3.9.0 Beta 1 for WordPress
- WooCommerce 3.9.1 for WordPress
- WooCommerce 3.9.2 Release Candidate 1 for WordPress
- WooCommerce 3.9.1 for WordPress

Description

WooCommerce is an open source e-commerce plugin for WordPress. An SQL injection vulnerability impacts all WooCommerce sites running the WooCommerce plugin between versions 3.9.0 and 3.9.1. Malicious actors (admins) having admin access, or API keys to the WooCommerce site can exploit vulnerable endpoints of /wp-json/wc/v3/webhooks and /wp-json/wc/v3/webhooks, and other

Mastercard Threat Intelligence

Payment Intelligence Reports

Emerging Fraud Tactics in Digital Payments and How They Are Evolving

MAY 2025

As digital payments grow, so do the tactics used by fraudsters. From AI-powered scams to synthetic identities, this topic explores how fraud tactics are evolving and what strategies can help mitigate rising threats.

Download PDF Report

High-Risk Merchant Trends and the Most Common Red Flags to Watch For

APRIL 2025

High-risk merchants are increasingly leveraging digital platforms, making it crucial to recognize emerging trends and red flags. From excessive chargebacks to suspicious transaction patterns, this topic dives into how to spot potential fraud and mitigate risk before it escalates.

Download PDF Report

Emerging Fraud Tactics in Digital Payments and How They Are Evolving

APRIL 2025

As digital payments grow, so do the tactics used by fraudsters. From AI-powered scams to synthetic identities, this topic explores how fraud tactics are evolving and what strategies can help mitigate rising threats.

Download PDF Report

High-Risk Merchant Trends and the Most Common Red Flags to Watch For

MARCH 2025

High-risk merchants are increasingly leveraging digital platforms, making it crucial to recognize emerging trends and red flags. From excessive chargebacks to suspicious transaction patterns, this topic dives into how to spot potential fraud and mitigate risk before it escalates.

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.

For more information, please reach out to [threat.intelligence@mastercard.com](mailto:threat.intelligence@mastercard.com)

