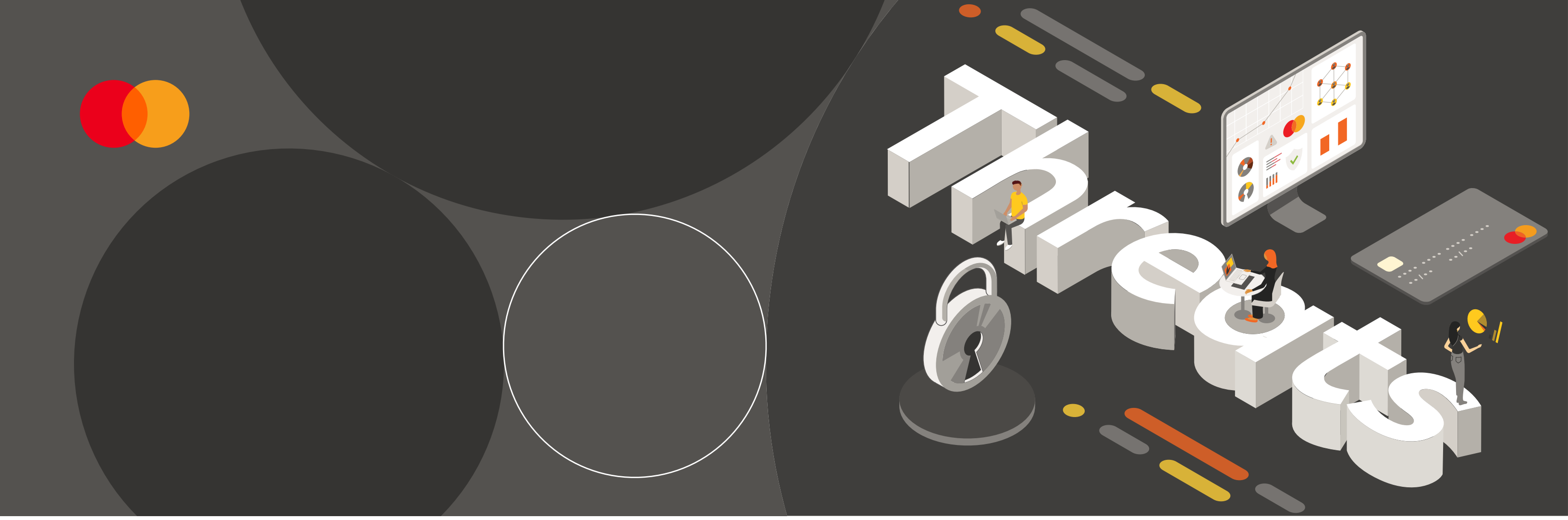


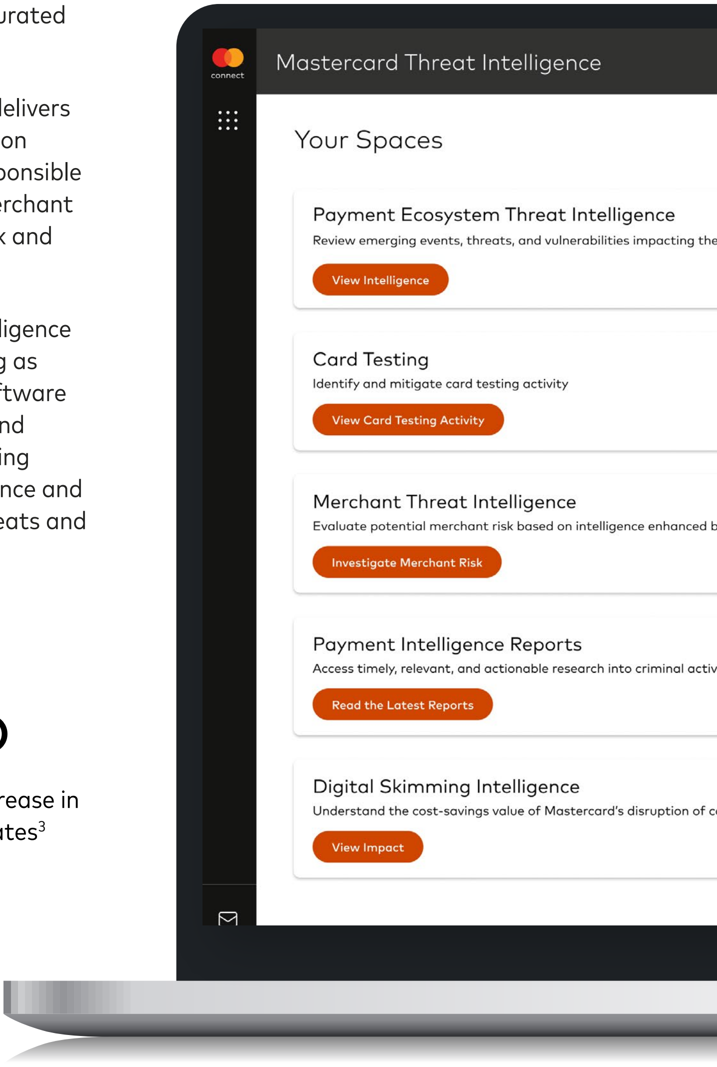
Stop emerging payments fraud faster with Mastercard Threat Intelligence

ACQUIRER DATASHEET ● SEPTEMBER 2025

Mastercard Threat Intelligence gives payment fraud and risk practitioners a curated view of emerging cyber threats across the payment ecosystem.

Built on Mastercard's unique network visibility and global threat expertise, it delivers targeted intelligence by collecting, analyzing and sharing actionable information through Mastercard Connect® — so teams can stay ahead of fraud. Those responsible for protecting payment acceptance, including Know Your Customer (KYC), merchant risk and compliance, can proactively prevent criminal activity, reduce cyber risk and strengthen their threat response maturity.

By expanding visibility into evolving payment threats, Mastercard Threat Intelligence allows teams to triage challenges such as merchants targeted for card testing as well as emerging fraud schemes. It provides insights into popular payment software vulnerabilities, digital skimming, and merchant domain activity, giving fraud and risk practitioners the information they need to take informed action. By enabling advanced payment threat intelligence to be shared across fraud, risk, compliance and cybersecurity functions, organizations can collaborate more effectively to threats and minimize fraud losses.



Mastercard Threat Intelligence

Your Spaces

Payment Ecosystem Threat Intelligence

Review emerging events, threats, and vulnerabilities impacting the

View Intelligence

Card Testing

Identify and mitigate card testing activity

View Card Testing Activity

Merchant Threat Intelligence

Evaluate potential merchant risk based on intelligence enhanced b

Investigate Merchant Risk

Payment Intelligence Reports

Access timely, relevant, and actionable research into criminal activ

Read the Latest Reports

Digital Skimming Intelligence

Understand the cost-savings value of Mastercard's disruption of c

View Impact

57%

of global fraud executives are notified of cyber breaches only after fraud losses begin[1]

59%

of cybersecurity leaders are critically understaffed in threat intelligence areas[2]

13%

year-over-year increase in payment attack rates[3]

[1] Datos Cyber Fraud Integration Survey, August 2025.
[2] ISACA. *State of cybersecurity, 2023 survey report*, 2023.
[3] Lexisnexis Risk Solutions. *Cybercrime report*, 2024.

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.

Card testing can negatively impact acquiring banks with fees and operational costs. Often a precursor to high-impact fraud, card testing is used by criminals to validate stolen or computer-generated card credentials and typically include a surge of low-value authorization attempts or a spike in declines. Mastercard Threat Intelligence informs teams when merchants in their portfolio are being targeted or suspected for card testing.

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 suspicious 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

Keep pace with evolving payment threats through curated, weekly intelligence built for merchant risk and compliance teams.

Stay informed with tailored updates highlighting relevant ecosystem risks, including high-risk e-commerce vulnerabilities and emerging merchant-targeted threats. Designed for non-cyber specialists, this curated feed delivers timely, actionable intelligence and insights. Payment risk teams gain visibility into recent threats and trends, with expert-level insights that allow them to coordinate with internal security teams without requiring 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 — including account data compromise and PCI-related vulnerabilities — with actionable guidance that can be used across the business. Organizations gain access to anonymized case studies, best practices and strategic recommendations that support confident reporting, cross-team collaboration and a more holistic approach to combating fraud.

Actionable, curated intelligence built for teams securing payment acceptance

Break down siloes to strengthen your fraud response

Mastercard Threat Intelligence bridges gaps between fraud and cyber operations — so you can build a more coordinated approach to managing merchant risks.

Proactively manage merchant risk

Powered by ongoing threat insights and automation, Mastercard Threat Intelligence continuously surfaces exposures impacting your merchant portfolio.

Act with precision, powered by Mastercard's insights

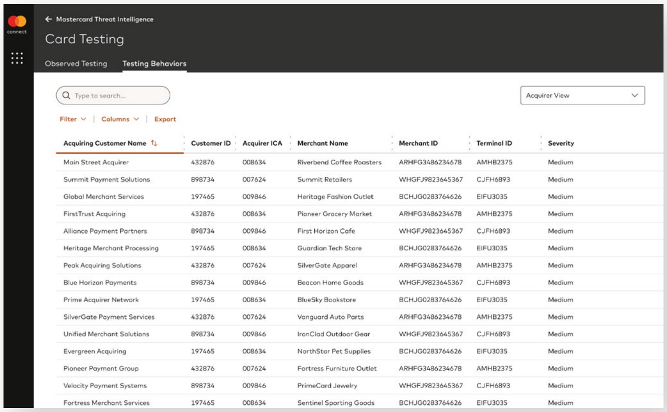
Get clarity on every threat response with intelligence built on Mastercard's global network data, unique visibility and decades of payments fraud expertise.

Extend your team without expanding it

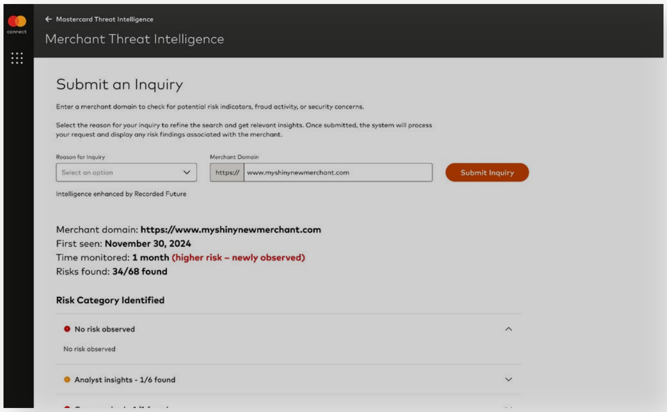
Scale your team with automation and expert insights, empowering faster investigations with existing resources.

Easy access through Mastercard Connect®

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



Acquiring Customer Name	Customer ID	Acquirer ICA	Merchant Name	Merchant ID	Terminal ID	Severity
Main Street Acquirer	432876	008634	Riverbend Coffee Roasters	ARHFG3486234678	AMHB2375	Medium
Summit Payment Solutions	898734	007624	Summit Retailers	WHGFJ9823645367	CJFH6893	Medium
Global Merchant Services	197465	009846	Heritage Fashion Outlet	BCHJG0283764626	EIFU3035	Medium
FirstTrust Acquiring	432876	008634	Pioneer Grocery Market	ARHFG3486234678	AMHB2375	Medium
Alliance Payment Partners	898734	009846	First Horizon Cafe	WHGFJ9823645367	CJFH6893	Medium
Heritage Merchant Processing	197465	008634	Guardian Tech Store	BCHJG0283764626	EIFU3035	Medium
Peak Acquiring Solutions	432876	007624	SilverGate Apparel	ARHFG3486234678	AMHB2375	Medium
Blue Horizon Payments	898734	009846	Beacon Home Goods	WHGFJ9823645367	CJFH6893	Medium
Prime Acquirer Network	197465	008634	BlueSky Bookstore	BCHJG0283764626	EIFU3035	Medium
SilverGate Payment Services	432876	007624	Vanguard Auto Parts	ARHFG3486234678	AMHB2375	Medium
Unified Merchant Solutions	898734	009846	IronClad Outdoor Gear	WHGFJ9823645367	CJFH6893	Medium
Evergreen Acquiring	197465	008634	NorthStar Pet Supplies	BCHJG0283764626	EIFU3035	Medium
Pioneer Payment Group	432876	007624	Fortress Furniture Outlet	ARHFG3486234678	AMHB2375	Medium
Velocity Payment Systems	898734	009846	PrimeCard Jewelry	WHGFJ9823645367	CJFH6893	Medium
Fortress Merchant Services	197465	008634	Sentinel Sporting Goods	BCHJG0283764626	EIFU3035	Medium


connect
← 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: Select an option

Merchant Domain: https:// www.myshinynewmerchant.com

Intelligence enhanced by Recorded Future

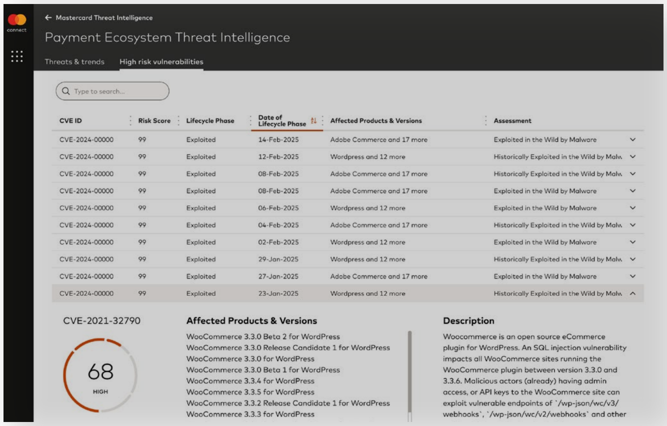
Merchant domain: **https://www.myshinynewmerchant.com**
First seen: **November 30, 2024**
Time monitored: **1 month (higher risk – newly observed)**
Risks found: **34/68 found**

Risk Category Identified

● No risk observed

No risk observed

● Analyst insights - 1/6 found


connect
← Mastercard Threat Intelligence
Payment Ecosystem Threat Intelligence
Threats & trends
High risk vulnerabilities
Type to search...

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 Malw
CVE-2024-00000	99	Exploited	08-Feb-2025	Adobe Commerce and 17 more	Historically Exploited in the Wild by Malw
CVE-2024-00000	99	Exploited	08-Feb-2025	Adobe Commerce and 17 more	Exploited in the Wild by Malware
CVE-2024-00000	99	Exploited	06-Feb-2025	Wordpress and 12 more	Exploited in the Wild by Malware
CVE-2024-00000	99	Exploited	04-Feb-2025	Adobe Commerce and 17 more	Historically Exploited in the Wild by Malw
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 Malw
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 Malw

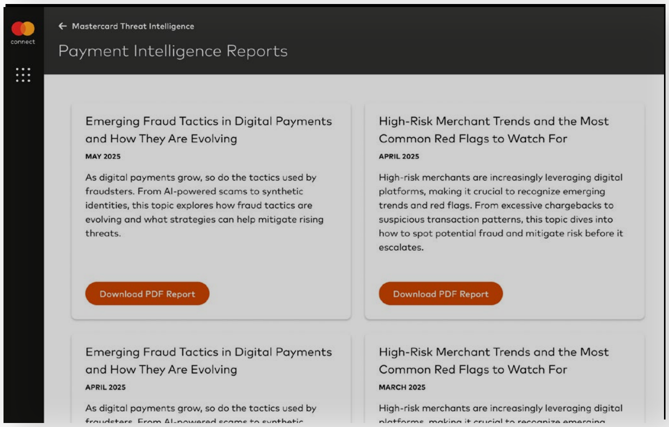
CVE-2021-32790

Affected Products & Versions

WooCommerce 3.3.0 Beta 2 for WordPress
WooCommerce 3.3.0 Release Candidate 1 for WordPress
WooCommerce 3.3.0 for WordPress
WooCommerce 3.3.0 Beta 1 for WordPress
WooCommerce 3.3.4 for WordPress
WooCommerce 3.3.5 for WordPress
WooCommerce 3.3.2 Release Candidate 1 for WordPress
WooCommerce 3.3.3 for WordPress

Description

Woocommerce is an open source eCommerce plugin for WordPress. An SQL injection vulnerability impacts all WooCommerce sites running the WooCommerce plugin between version 3.3.0 and 3.3.6. Malicious actors (already) having admin access, or API keys to the WooCommerce site can exploit vulnerable endpoints of `/wp-json/wc/v3/webhooks`, `/wp-json/wc/v2/webhooks` and other


connect
← 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.

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.

Emerging Fraud Tactics in Digital Payments and How They Are Evolving
APRIL 2025
As digital payments grow, so do the tactics used by

High-Risk Merchant Trends and the Most Common Red Flags to Watch For
MARCH 2025
High-risk merchants are increasingly leveraging digital

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.