

# CARD TESTING PREVENTION

**COMPLETE GUIDE**

**How To Detect  
and Prevent Card  
Testing Attacks**

# Card Testing Attacks

Card testing is a method used by fraudsters to validate stolen credit card information, posing financial and reputational risks for e-commerce and retail businesses. These attacks can be disruptive and may indicate broader security vulnerabilities.

**\$43b**

Global credit card fraud losses by 2026

**This guide explains key elements of card testing, including how attacks work, the impact on merchants, and how to prevent card testing to maintain a secure customer journey.**

## What is Card Testing?

Card testing is a fraud tactic where criminals use stolen credit card information to verify whether cards are active and have available funds. This is typically done by initiating small transactions or authorizations that may go unnoticed by the cardholder. These transactions are often conducted using automated scripts, enabling fraudsters to test thousands of cards quickly.

## Why Card Testing Prevention?

Once valid cards are identified, they can be resold on the dark web, used for larger purchases, or exploited for other fraudulent activities. Card testing often flies under the radar, especially in systems lacking robust fraud prevention measures. If card testing is left unchecked, it can lead to increased chargebacks and fraud losses.

**85%**

**MRC members experiencing card testing attacks**

# How Card Testing Works

Fraudsters employ several techniques to test stolen or generated card details. Understanding these methods helps businesses anticipate vulnerabilities and implement stronger defenses.



## Small Value Transactions

Fraudsters attempt low-value payments on stolen cards. These transactions are less likely to raise alarms with merchants or cardholders but can confirm whether a card is active.

## Authorization Requests

These queries verify if a card has enough funds without completing a transaction and often without appearing on cardholder statements, which gives fraudsters an opportunity to act undetected.

## Automated Scripts and Bots

Fraudsters use automation to test hundreds or thousands of cards quickly. By rotating through different card numbers and endpoints, they exploit weak defenses.

## Targeting Vulnerable Endpoints

Fraudsters often target e-commerce sites, donation pages, and other platforms with low-friction payment setups to test and validate stolen cards.

# Impact of Card Testing Fraud

Card testing fraud has significant consequences beyond financial losses, affecting customer trust and disrupting business operations.



## Financial Losses

Businesses incur financial penalties such as chargebacks, dispute fees, and costs from failed or fraudulent transactions. These cumulative expenses can severely strain resources and decrease profitability over time.

## Reputation Damage

Customers expect businesses to protect payment information. Card testing fraud can damage customer trust and harm a brand's reputation, making it harder to retain existing customers and attract new ones.

## High Processing Fees

Frequently failed card transactions from testing signals risk for payment processors, leading to higher transaction fees, lower acceptance rates for legitimate payments, and further reputation damage over time.

## Infrastructure Strain

Automated attacks generate excessive traffic, overwhelming payment gateways, APIs, and servers. This disrupts legitimate transactions, causing downtime, slower service, and poor user experiences during peak times.

## Increased Fraud Risk

Card testing indicates weak defenses, making businesses targets for future fraud. Vulnerable platforms attract fraudsters, increasing the chances of repeated and more sophisticated attacks.

# Emerging Trends in Card Testing Attacks



Card testing fraud is constantly evolving as fraudsters adapt to security measures. Understanding these trends is vital for businesses to prevent potential attacks.

## 1 AI-Driven Bot Attacks

Fraudsters use AI-powered bots for card testing, mimicking human behavior to evade detection. These bots operate in "low and slow" modes, testing small numbers of cards over time to blend in with legitimate users while targeting multiple platforms for higher success.

## 2 Seasonal Spikes in Attacks

High-traffic times create opportunities for card testing, as the surge in legitimate transactions can hide fraudulent activities. Merchants often experience an increase in low-value transactions during these periods, signaling potential card testing.

## 3 Exploitation of New Payment Methods

As businesses adopt mobile wallets, buy-now-pay-later services, and cryptocurrency, fraudsters exploit vulnerabilities due to weaker security measures in these payment systems, making them attractive for testing stolen card information.

# Emerging Trends in Card Testing Attacks



## 4 Increased Focus on Donation Platforms

Donation platforms face card testing threats due to low-friction payment processes, allowing fraudsters to exploit minimal oversight. This trend is especially worrying for nonprofits that may not have the resources for strong fraud prevention.

## 5 Multi-Platform Attacks

Modern fraudsters leverage multiple platforms to test and validate cards. They may use one platform to test cards with small transactions and another to make larger fraudulent purchases once the card is validated. This distributed approach makes it harder to track and stop fraud.

Learn how to prevent card testing attacks with Spec!

[LEARN MORE](#)



# How to Identify Card Testing Fraud



Early detection of card testing fraud is crucial to reduce its impact, as these attacks show identifiable patterns and behaviors that businesses can monitor.

- 1** **Transaction Anomalies**  
Spikes in failed or low-value transactions, especially in rapid succession, are common indicators. Fraudsters use these small transactions to test multiple cards quickly.
- 2** **Suspicious Details**  
Transactions linked to nonsensical or fake customer names, email addresses, and billing details often point to fraudulent activity.
- 3** **Unusual Patterns**  
Multiple payment attempts originating from the same IP address, device, or geographic location can indicate automated activity.
- 4** **Error Codes and Logs**  
Monitoring API logs for patterns like repeated 402 errors or similar failure codes can reveal card testing attempts in progress.
- 5** **Velocity Indicators**  
High volumes of requests targeting payment endpoints, such as multiple card additions or transactions from a single source, are red flags for fraud.

# How To Stop Card Testing

Stopping card testing fraud involves businesses using multiple security layers that work together to deter attacks while ensuring a smooth experience for legitimate users.

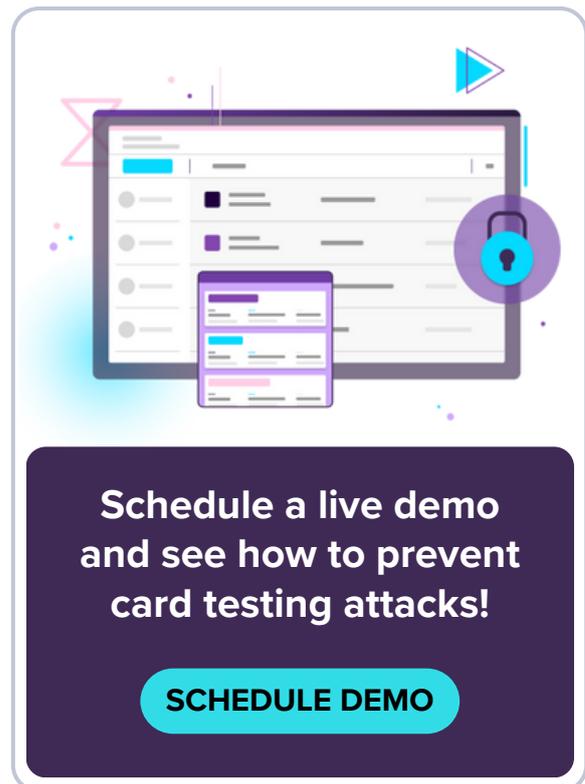
✓ **Strengthen Authentication Measures:** Adding CAPTCHAs or multi-factor authentication (MFA) creates additional hurdles for fraudsters attempting to exploit your platform. These measures block automated scripts, which minimizes risk.

✓ **Set Rate Limits:** This restricts the number of actions that can be performed by a single user, IP address, or device within a set time frame. It slows down automated attacks and makes it harder to validate multiple cards quickly.

✓ **Implement Behavioral Analytics:** Advanced fraud prevention tools, like Spec Customer Journey Security, analyze user behavior across the entire customer journey. By focusing on behavior, this method utilizes subtle, “low and slow” attacks that would otherwise evade traditional defenses.

✓ **Block Suspicious IPs and Devices:** Tracking IP addresses and device fingerprints associated with fraudulent activity allows businesses to block future access from these sources.

✓ **Secure Payment Endpoints:** Requiring login credentials or session validation before allowing access to payment forms or other sensitive areas reduces exposure to card testing attacks.



# Best Practices for Card Testing Prevention

Preventing card testing requires a comprehensive strategy involving technology, teamwork, and continuous vigilance.



## Leverage Fraud Detection Solutions

Implement solutions like Spec Customer Journey Security to monitor real-time customer interactions and detect advanced fraud patterns using Spec's 14x richer data.



## Collaborate Across Internal Teams

Fraud teams analyze anomalies in real-time, security teams integrate prevention tools in the customer journey, and product uses invisible protections for a seamless experience.



## Focus on Fraud Data Enrichment

Combine data points like IP addresses, device details, and behavior patterns to create detailed user profiles for accurate risk assessments and faster responses.



## Stay Proactive Using Advanced Tools

Continuously update fraud detection systems to keep pace with evolving attack methods. Regularly train teams to recognize new fraud indicators.

# Card Testing Fraud Prevention: Payments Platform

## Payments Platform Situation

The payments platform faced fraud challenges due to the absence of validation or verification checks. The main vulnerability was fraudsters conducting low-dollar card tests across time zones. Despite dedicating significant resources, the team struggled to combat these attacks and ultimately lost the battle against card testing fraud.

**99%**

Reduction in  
Attack Pressure

**92%**

Reduced Card  
Declines

**95%**

Authorization  
Rates Restored

## Spec's Advanced Solution

Utilize extensive data insights and a flexible platform to create detailed workflows for detecting fraud while protecting legitimate users. Rather than static rules, Spec employs dynamic protections that adapt to fraudsters' tactics. A key tool is honeypots — strategic traps that entice fraudsters to reveal their methods without notifying them of their failure, enabling Spec to gather intelligence on their evolving strategies.

**Take a product tour of  
the Spec platform!**

[TOUR SPEC PLATFORM](#)



# Prevent Card Testing With Customer Journey Security

## What is Customer Journey Security?

**Spec Customer Journey Security** goes beyond traditional fraud tools by monitoring and analyzing every user interaction throughout the journey. This comprehensive approach provides deeper insights and allows for more proactive prevention to stop account takeovers before they happen.

## How Does It Work?

- ✓ **Journey Data™ Collection:** Captures 14x more data points than traditional fraud systems, offering a detailed view of user behavior at every touchpoint of the customer journey.
- ✓ **Behavioral Modeling and Entity Graphs:** Enables accurate identification of legitimate users versus fraudulent activity modeling behavior across sessions, devices, and IP addresses.
- ✓ **Automated and Invisible Protections:** Uses techniques like honeypots and redirects to block fraud without affecting the experience of legitimate customers.



# Why Choose Spec Customer Journey Security?

## What Makes Spec Different?

Spec stands out among fraud prevention companies due to our comprehensive approach, advanced technology, and access to 14x more data than traditional fraud systems.

- ✓ **Unmatched Data Coverage:** Collects 14x more data than traditional fraud tools for deeper insights and broader coverage.
- ✓ **Proactive and Adaptive Detection:** Uses real-time behavioral analysis to detect and respond to evolving threats before cause harm.
- ✓ **Invisible Protections:** Secures the customer journey without impacting the experience of legitimate users and customers.
- ✓ **Easy Integration:** Seamlessly integrates with existing systems, ensuring a smooth deployment process and effortless integration.
- ✓ **High Accuracy in Risk Decisioning:** Minimizes false positives and operational inefficiencies, providing precise fraud detection.

The screenshot displays the 'Entity Spotlight' dashboard for the user 'charlie\_demo@specprotected.com'. The dashboard is divided into several sections:

- Entity Spotlight (All Time):** Shows the entity value 'charlie\_demo@specprotected.com', entity type 'Email', first seen '10/02/24, 7:04:58 PM', linked sessions '22', and linked entities '32'.
- Entity Map (Last 90 Days):** A map showing the entity's location in Spain, with a red pin on the Iberian Peninsula.
- Transaction Highlights (Last 90 Days):** A list of transactions with icons and values:
  - 812.18 (Purchases Made: 3)
  - 1,431.20 (Refund Ratio: 166.7%)
  - 0.00 (Chargeback Ratio: 0%)
- Linked Entities (Last 90 Days):** A table showing 'Total Results: 32'. The table has columns for 'Entity Type', 'Details', and 'Shared Sessions'. The details for the first entry include: Postal Code: 28022, Country: es, and Street 1: Avenida de Maria 2c.
- Entity Labels (Last 90 Days):** A list of labels with checkboxes:
  - Linked to Reshipper
  - High Refund Ratio
  - Multiple Addresses
  - Linked to fraud by Spec ID

# Card Testing Prevention You Can Trust With Spec

At Spec, we understand trust is essential. That's why the Spec Customer Journey Security platform is engineered with the most stringent security, compliance, and privacy standards in mind.



Spec's platform not only meets industry standards but also ensures a seamless, secure user experience. By adopting an advanced card testing prevention solution, companies stay ahead of sophisticated fraud tactics and safeguard revenue.

An illustration showing a user interface with a card, a lock icon, and a dollar sign, representing a secure transaction process. A play button icon is also present, suggesting a demo or video content.

**Ready to  
prevent card  
testing attacks?**

[REQUEST DEMO](#)

