Solution guide

Card Testing

READ ON TO FIND OUT MORE →

cybersource
A Visa Solution

Contents

Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa Inc. does not make any warranty or representation as to the completeness or accuracy of the Information within this document, nor assume any liability or responsibility that may result from reliance on such Information. The Information contained herein is not intended as legal advice, and readers are encouraged to seek the advice of a competent legal professional where such advice is required.

What is card testing?

Fraudsters use card testing to determine the validity of stolen or fraudulently obtained card details. They attempt multiple purchases on an eCommerce website like yours (often using a botnet for speed and scale). If a transaction is approved, they know they can continue to use the card. If a card has already been canceled by its owner, authorization will be declined, and the fraudster will move on to the next card. This process could lead to increased authorization fees and processing shutdowns for targeted merchants.

Our risk analysts have identified card testing as a prevalent type of fraud affecting small and medium businesses in 2022. Card testing is one of the most impactful types of fraud for small and mid-size businesses. Unlike regular instances of chargebacks, the serious effects of a card testing attack can cause you to lose your business.

Fraudsters deliberately target businesses that are unlikely to have an internal fraud team. We find that customers often turn to Cybersource after suffering a card testing attack they were unprepared for because they assumed they were too small to attract the attention of fraudsters.

The best way to fight card testing is to be proactive, rather than reactive, with your fraud protection.

By the time you're aware that you've been hit by card testing, it might already be too late.

Use cases

Without Fraud Management Essentials

Cybersource's risk analysts have found that a card testing attack typically looks like this:

Day 1

The fraudster submits thousands of transactions. Approved orders could start to ship out, resulting in lost product.

Day 2–30

Card issuers become aware of what's happening and ask the merchant's acquirer to shut down processing. The merchant must supply proof of a mitigation strategy to begin processing transactions again. (This could also potentially occur the same day as the attack.)

The merchant is charged significant authorization fees by their gateway and acquirer.

For example, a merchant who usually pays $40/month in authorization fees could see a charge of $15,000 or more.

Day 2–120

Chargebacks start to roll in with associated fees because transactions were not reversed during the attack.

Ongoing

The merchant experiences brand and reputational damage due to accounts being compromised.

With Fraud Management Essentials

While no tool can completely prevent fraud, Fraud Management Essentials can limit your risk of experiencing the serious effects of card testing.

Get set up right away and begin protecting your business from fraud.

- Learn how to craft a fraud strategy and implement it at your own pace with our Fraud Training Modules.
- Pre-configured rules and settings help you get started quickly.

Velocity rules, negative lists, and other types of rules are built into Fraud Management Essentials to equip you to prevent card testing.

Tips

5 Tips from Cybersource risk analysts: Protecting against card testing

1

Perform risk reviews.

Keep a close eye on your traffic and review transactions on a regular basis.

Fraudsters often target the point when cardholders add payment methods to their online accounts on merchant sites. Be sure to evaluate your web setup to ensure plugins, apps, and other potential points of weakness are up to date and secure.

2

If you accept donations or other custom payment amounts, set a minimum.

In a card testing attack, fraudsters aim to validate if a card is good without the cardholder noticing and reporting it. The smaller the charge, the less likely it is to attract attention or result in a chargeback. Transactions can often be $5 or less. Set a minimum value that is as high as possible while still being appropriate for most donors.

3

Be vigilant and identify anomalies early on.

If you see an unexpected spike in average daily transactions, look into it.

A sudden increase in the number of card declines can signal that your business is being targeted.

Have a variety of velocity tools that track not only transaction totals, but also other specific data elements (including email, IP address, device fingerprint, etc.).

4

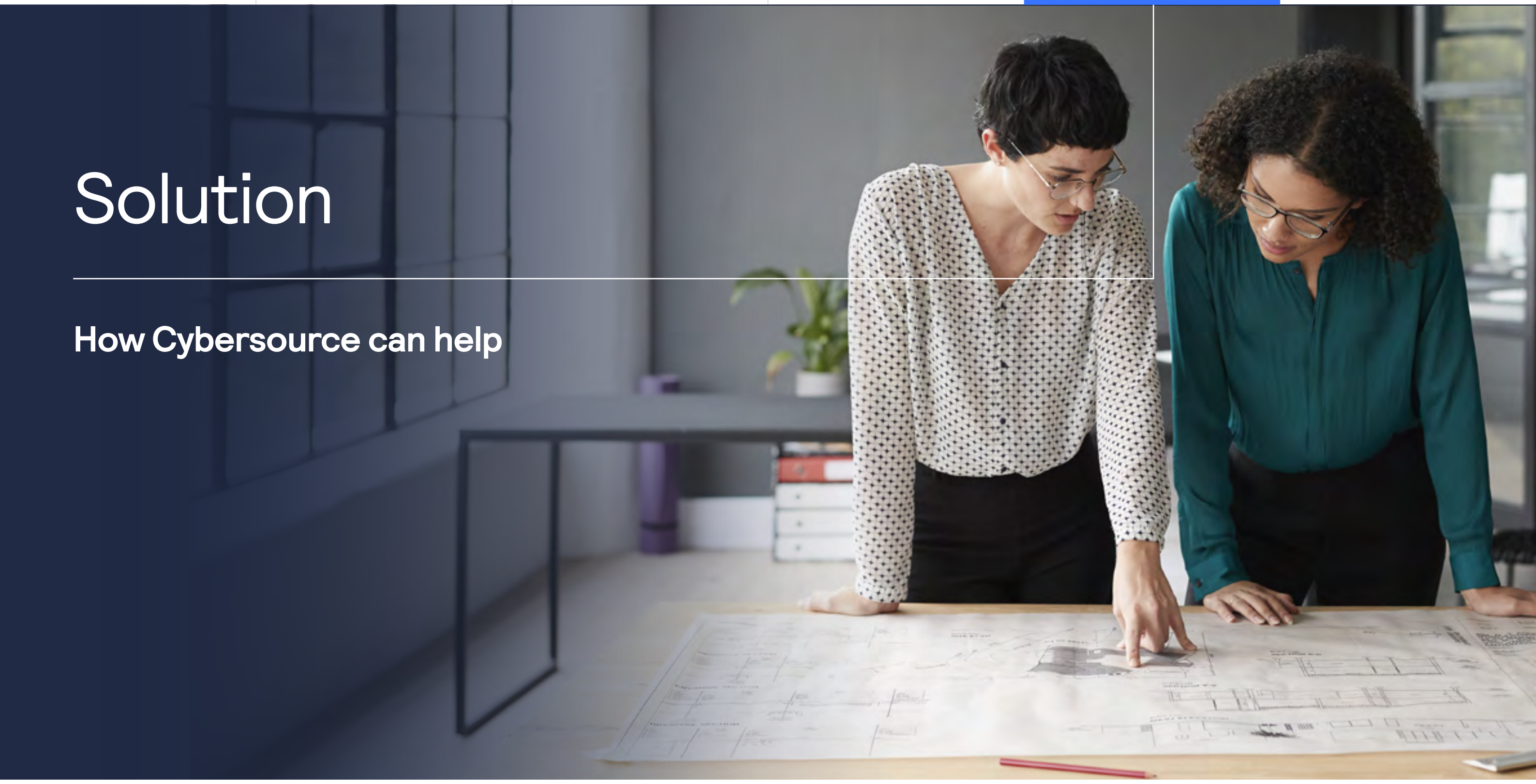
Consider implementing some type of CAPTCHA into your checkout flow.

This technology has improved in recent years and can produce much less friction to your customers than previous versions

5

Make sure you have a fraud tool in place.

A fraud protection tool on your website is important because it helps to prevent fraudulent transactions and protect your business from financial loss and reputational damage. It's like having a security guard for your online store, who can monitor and flag suspicious activity before it becomes a problem.



Solution

How Cybersource can help

Fraud Management Essentials is our streamlined solution that helps prevent card testing and other common fraud attacks.

Get started right away with preconfigured settings.

Gain control of your fraud defense. You don't need to be an expert to protect yourself.

Reduce fraud without adding friction at checkout with customer-friendly protection.

Easy to use but built on the strength of Visa and Cybersource's powerful data and machine learning platform.

Make sure your business is prepared

Your business could be a target of card testing. Make a plan to proactively protect it from costly brand and reputational damage.

Implement a fraud solution that fights card testing to help avoid:

- Impacts on your payment processing and chargeback rates in the short term.
- Significant business costs over the long term.

Ready to get started?

Get started now with

> Fraud Management Essentials

cybersource
A Visa Solution