clearsale

6 Fundamentals to Protect Your e-Commerce Business From CNP Fraud

By **Rafael Lourenco**, EVP at **ClearSale**

No e-commerce retailer wants to worry about whether a fraudster is preparing to launch an attack against their business. But card-not-present (CNP) fraud is on the rise, and retailers are right to worry. In fact, nearly 75% of retailers surveyed by Experian cite fraud as a growing concern.

The impact of CNP fraud is serious. Every $1 of fraud costs merchants $2.94 in additional fees and expenses. If you're an e-commerce business owner, this means it's not enough to focus on increasing revenue, delivering exceptional products and services, and developing long-term customer relationships. You must also be thinking about how to minimize your fraud risk.

While there are many different types of e-commerce fraud protection solutions available on the market, the best place to start is to make sure you have certain key fundamentals in place. From there, you can layer on solutions as it's appropriate for your unique business.

1. Protect Your Customer Data

E-commerce fraud generally begins with someone accessing stolen credit card data. If you can prevent that from happening in the first place, you've thwarted the fraudsters in their tracks.

Payment Card Industry Data Security Standards (PCI DSS) ensure all sensitive consumer data is stored and transmitted in a secure environment. Any merchant that accepts credit card payments must be PCI DSS compliant – but PCI DSS compliance can be complicated. Choosing an e-commerce platform that incorporates PCI DSS compliance into existing payment processes will make this significantly easier.

2. Require Strong Passwords

Consumers generally want their online shopping experiences to be as easy and hassle-free as possible. They may know that creating accounts and choosing good passwords are for their own protection, but even so, many consumers still resist this – favoring simplicity over security.

As a merchant, it's your duty to do what's right and protect your customers – regardless of what they tell you they want. The truth is that simple passwords are easy to hack, and no consumer wants their account to be hacked.

Help your customers protect their data and reduce the risk of account takeovers by setting stringent password requirements. Cybersecurity experts recommend passwords include at least a minimum of eight characters with a combination of upper- and lowercase letters, numbers, and special characters.

3. Improve Your Website Security

Nearly 66% of consumers say e-commerce security protocols make them feel protected when making a purchase. Fortunately, website security doesn't have to be complicated.

First off, make sure to regularly update your systems and apply security patches as soon as they're released. You should also make sure your website has a Security Socket Layer (SSL) certificate. This security protocol encrypts the transmission of information between your website server and your end user – which can help protect your customer's personal data from being stolen while it's being transmitted. And finally, refrain from using website extensions, plugins, or themes unless they come from reliable developers and have been thoroughly tested before going live.

4. Verify Customer Identities

clearsale

Although fraudsters will go to great lengths to conceal their identities and pose as legitimate customers, you should nonetheless implement some basic identification strategies into your checkout process. This includes requiring the Card Verification Value (CVV) and utilizing the Address Verification System (AVS).

The CVV (or CID, on some cards) is a three-number code on the back of a credit card (or four-number code on the front of American Express cards) intended to help verify a user is physically holding the card.

AVS matches the numerical part of an address that a credit card company has on file for the cardholder with the address the customer has input during the checkout process. The closer the match, the more confident you can be that the customer is the true cardholder. You can also decide what level of match to require; some merchants choose to automatically reject all mismatched orders, while others choose to review mismatched orders on a case-by-case basis.

5. Keep Paperwork Organized and Accessible

In the event an approved transaction results in a chargeback, you can dispute the chargeback if you think you can prove that the order was not in fact fraudulent. To do this successfully, you need thorough and accurate documentation of the transaction. This includes details on:

- Customer order history
- Shipping and delivery confirmations (or proof of download, if the product is a digital good)
- All email, phone, or written communications with the customer

Standard processes for saving transaction records will help ensure you can quickly retrieve all the information you need. It's also helpful to stay familiar with chargeback processes, since policies and guidelines can change.

6. Add Specialized Fraud Detection

Many small businesses opt to rely on the fraud protection options available in their e-commerce platform. While this may be a relatively inexpensive approach, it also may not be enough to protect your business from savvy fraudsters who have an amazing amount of tricks up their sleeves.

One alternative is to dedicate someone on your e-commerce team to review any questionable transactions that are placed. And yet as you grow, this resource-intensive approach can be difficult to sustain.

At some point, it will make sense to incorporate a more robust, outsourced fraud prevention solution that provides the protection you need and frees up your in-house resources to focus on more strategic growth endeavors. The right solution for your business will include fraud protection tactics specifically designed to address any unique risks in your industry and to accommodate your own internal business processes and priorities.

Ultimately, protecting your business and your customers from e-commerce fraud is achievable – whether that means fine-tuning your back-end systems to prevent fraud or educating your customers about emerging fraud risks. Make sure you have your fundamentals covered, and layer in more advanced solutions as you grow. You'll likely find these simple changes can make the biggest impact.

Author:

Rafael Lourenco is Executive Vice President and Partner at ClearSale, a card-not-present fraud prevention operation that helps retailers increase sales and eliminate chargebacks before they happen. The company's proprietary technology and in-house staff of seasoned analysts provide an end-to-end outsourced fraud detection solution for online retailers to achieve industry-high approval rates while virtually eliminating false positives.

Follow on twitter at @ClearSaleUS or visit www.clear.sale.