PayPal

5 steps to help prevent fraudulent payments

Managing your risk

Fraudulent payments and activity can affect your online business and sales. By putting the right tools and processes in place, you can minimise the risk and help keep your business and customers secure – reducing your chances of chargeback fees and lost revenue.

How fraudsters operate

Generally, online fraudsters use two methods to steal money:

Account takeover:

A common scheme involves fraudsters sending emails to trick customers into revealing usernames and passwords of their retail account. Next, they log in, change passwords, and make unauthorised purchases.

Identity theft:

Despite businesses taking precautions, fraudsters still manage to hack into databases for personal information. Hackers often sell credit card numbers to other fraudsters, who open online retail accounts and use the stolen numbers to shop, without the victim knowing.

The five steps to preventing fraudulent payments

Monitor transactions and reconcile your bank accounts daily

Nobody knows details about your business as well as you – such as biggest spenders and buying patterns. Monitor your accounts for red flags including inconsistent billing, shipping information and physical location of customers.

Consider setting limits

Set limits for the number of purchases and total currency value you'll accept from one account in a day. It can help keep your exposure to a minimum should fraud occur.

Require the card verification value (CVV)

PCI rules prevent storage of a customer's CVV along with the credit card number and card owner's name. That's why it's so effective – it's virtually impossible for fraudsters to obtain unless they've stolen the physical card. Most processors include a tool that requires CVV as part of their checkout templates. Use one.

Get tougher with password requirements

Hackers employ sophisticated programs that can run through all versions of a password. Current best practices call for at least an eight-digit alpha-numeric password that requires at least one capitalisation and special character.

Keep your platforms and software up to date

Make sure you're running the latest version of your operating system (OS). OS Providers continually update their software with security patches to protect you from newly discovered vulnerabilities, plus the latest viruses and malware.

An important note about your anti-virus software

It's best practice to install and regularly update *business-grade* anti-malware and anti-spyware. Free, consumer-strength versions tend to not be sufficient. If your site is hosted on a managed solution, automatic security patches help ensure any vulnerabilities are quickly resolved.