IS FRAUD HURTING YOUR BUSINESS? HERE ARE 10 WAYS TO HELP GUARD AGAINST IT

Fraud is an inevitable part of running a business. Just as there are daily opportunities to delight your customers and drive new growth opportunities, there are also criminals waiting in the wings with their own agenda.

They may use counterfeit cards in-store, or more likely try to defraud you online by using card details stolen from legitimate cardholders. So-called card-not-present (CNP) fraud – which includes phone and mail order as well as internet-based scams – accounted for 76% of total fraud losses in 2018, exceeding £506m. E-commerce fraud alone reached nearly £400m, according to UK Finance.[i]

There are arguably more opportunities for the scammers to trick small businesses online then in face-to-face scenarios. That's partly because of the anonymising effect of the internet: your staff can't check visually to see if someone is acting suspiciously. It's also easier because stolen payment card data is readily available for fraudsters to buy on the cybercrime underground. Some sellers even provide money back guarantees if the card in question turns out to have been blocked by the cardholder. Prices fluctuate massively depending on demand but one report from 2018 claimed that debit cards were selling for as little as £6.30.[ii]

Time to fight back

Fraud can be a drain on small businesses. Transactions purchased with stolen card details will result in chargebacks to the business and can damage customer loyalty. But add too many fraud checks, especially online, and you may also put your customers off buying altogether.

The answer lies with a mixture of improved staff training, and technical measures. Here are 10 tips to help tackle the spectre of fraud.

1) **Look out for counterfeit cards**
   Some fraudsters may try to trick staff in your store, with a counterfeit or altered card. Sales assistants should be trained to spot some of the tell-tale signs, including characters and numbers that appear crooked, unevenly spaced or otherwise unusual; a smudged or altered signature; a scratched/destroyed magnetic stripe; a damaged or dull hologram; or first numbers that don't match the card brand's typical format (American Express = 3, Visa = 4, Mastercard = 5, Discover = 6).

2) **Watch out for suspicious behaviour**
Staff can also be a great first line of defence against fraud by spotting the signs of a possible scammer. They may look nervous, try to shop just after a store opens or just before closing, have a damaged card to bypass magstripe/chip and PIN protections, or even try to pay without a card at all but simply a number.

3) **Detect suspect purchasing behaviour**
Fraudsters will often buy large numbers of expensive items – potentially way more than your usual transaction amount. These items may appear completely random in terms of size, colour and type. If a purchase was accepted, they may return to the store later to buy another batch of items. This is true of both bricks and mortar and online purchases.

4) **Spot multi-channel fraud**
Sometimes a fraudster will make a payment over the phone/online using a stolen card number and then request to collect the goods via a courier service, or friend/relative – because their address doesn't match the legitimate cardholder's. They may even buy online and look to pick-up in store, hoping to trick staff by claiming they've forgotten the physical card used to purchase. Both tactics should ring alarm bells.

5) **Follow PCI DSS**
All merchants that accept card payments need to follow the Payment Card Industry Data Security Standard (PCI DSS) guidelines. These have been designed to improve the security of your card processing environment and reduce the chance of fraud. For those concerned about the time and costs associated with compliance, consider adopting payment technology certified with P2PE v2, a PCI encryption standard which scrambles card details when they're entered into your terminal. Using this kit can reduce the compliance burden.

6) **Keep your IT systems up-to-date and secure**
Criminals are always looking for ways to steal the customer card data that can then be used to carry out fraud, and online attacks are a popular method. By keeping all your IT systems regularly patched (ie on the latest, most secure version) and secured with anti-malware protection, you stand the best chance of keeping these attacks at bay. Regular testing of your e-commerce system will also reveal any new vulnerabilities that may appear.

7) **Don't forget to use strong, unique passwords**
Enhance security further by ensuring there's no easy way for attackers to guess or crack open your IT administrator accounts – which could give them access to customer card data. The most secure method is two-factor or multi-factor authentication (2FA/MFA), which could mean using a fingerprint reader, facial recognition or one-time passcode to unlock accounts. Another option is to use a password manager to securely store all of your log-ins. This means you can create long, unique and hard-to-guess or crack passwords.

8) **Train staff to spot suspicious emails**
Hackers often use phishing emails to get a foothold into e-commerce environments. These are spoofed to appear as if coming from a legitimate source, and encourage the user to click on a link or open an attachment, which will either download malware or take them to a malicious page to enter in their log-ins. The best form of defence for this is training staff how to spot these emails.

9) **Use CSC/AVS checks**
A simple way to validate online users is checking the last three numbers on your customer's signature strip (CSC, CV2, CVV) and the numbers in their address (AVS).

10) **Switch on 3D Secure for online checks**
Implement 3D Secure authentication on your website. This will not only help to reduce online fraud but it's a requirement under the new PSD2 payment rules. Enhance these checks by partnering with a payment provider (PSP) that also runs background checks.

To find out more information on all of these tips, your payment service provider should be able to offer you practical advice on best next steps. The FSB Payments team is waiting for your call.

0808 301 9639

Monday-Friday: 9am-6pm

[i] UK Finance, https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf
[ii] Moneywise, https://www.moneywise.co.uk/news/2018-03-21%E2%80%8C%E2%80%8C/how-much-your-data-worth-hackers

WFIP005 12.19

fsb Payments