Elavon

# The ultimate guide to Security

Brought to you by Elavon,
the payments specialist

Version 01

# Contents

## Brought to you by Elavon, the retail payments specialist

# Introduction

*by Candice Pressinger, Director of Customer Data Security, Elavon Europe*

## Security. Sounds dull, right?

Too many ambitious businesses still think so. “I’ll get around to it.” “It’s too expensive.” Or my personal favourite: “We’re too small to be targeted.”

Here’s the truth: fraud doesn’t care how big you are.

More importantly, great security provides more than great protection for your business: it also performs for you.

It optimises what you’re doing, keeping your business lean, fast and competitive in a market where every click, every customer who walks through your door and every booking counts.

If you want to grow as a business, you can’t ignore it. You face the triple threat of big financial penalties; huge loss in confidence and trade; and by not optimising you lose revenue.

Let’s break that down a bit further.

## 01

**Breaches = big fines**

From May 2025, fees for non-compliance with PCI standards will be levied at up to $25,000 per month (see the PCI non-compliance fees box for more details). You might be thinking you’re too small for that kind of treatment, but the penalties for data breaches are eye-watering. This is just the fee for non-compliance – before anything actually goes wrong.

## 02

**Breaches = broken trust**

If you suffer a data breach, would your customers return? According to a recent report, 70% of consumers say they would stop doing business with a brand after a data breach. Can you afford to lose 70% of your business?

## 03

**No optimisation = lost revenue**

Fraud filters set too tight? Say goodbye to good customers. No local payment options? Expect high cart abandonment rates. Every percentage of conversion matters. Good security products and behaviours not only reduce the threat you face, they also optimise what you’re doing.

Fraud control should never come at the cost of your best customers.

But many businesses are already aware of the dangers.

Our own research shows that more than a fifth (21%) of small and medium-sized businesses are concerned about both fraud and data security. Meanwhile, 71% are concerned about costs. And as we've already discussed, fraud and costs go hand in hand.

That's why we've produced this guide. Educate yourself and your team to help in the battle against the threat of fraud. Use security to not only protect yourself, but optimise what you're doing – improving customer satisfaction and driving up growth in the process.

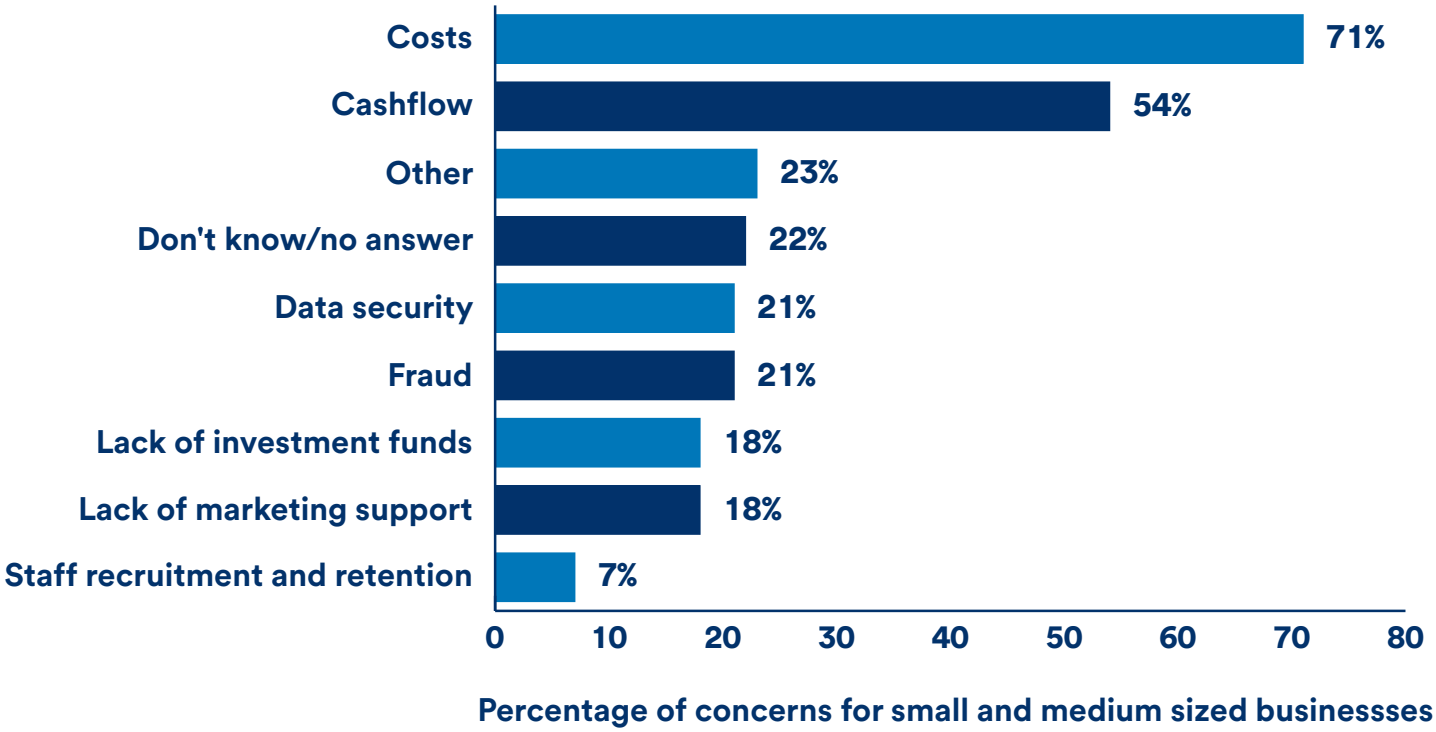
Security might be alarming, terrifying even. But together we can stay ahead and defeat the threat. And it certainly isn't boring.

In a survey of 510 small and medium-sized businesses, we asked what their top three concerns were for the coming months.

Costs came out top, with 71% of businesses ranking it in their top three, followed by cashflow at 54%.

Data security and fraud were both in the top three for a fifth of all businesses.

We understand your pain. We've got your back.




*Source: Yonder conducted an online survey of 510 owners or directors of small and medium sized businesses with a company size of up to 249 people, in the UK in April 2025. The sample was designed to give a spread of businessess across the UK and across sectors, and with quotas set on business size to represent the views across a range of businesses. The data was weighted to reflect Government statistics on UK business size by employee numbers. Yonder is a founding member of the British Polling Council and abides by its rules.*

# Chapter 1:
# Security and fraud threats in the current era

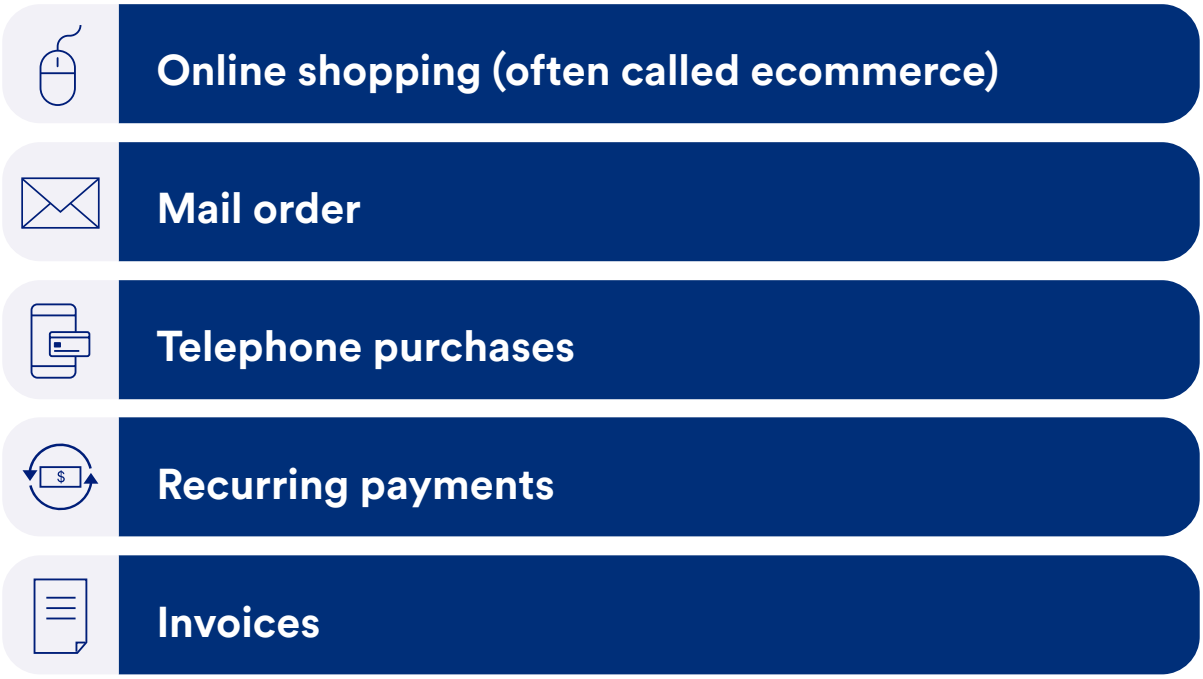
If you don't know how you're likely to be attacked, how can you prepare your defence? Understanding some of the most common threats you might encounter in your day-to-day business life – and your personal life – can help you prevent the unimaginable happening.

It's a fast-changing world, especially with the capabilities offered by generative AI. But take heart in knowing that more fraud is detected and stopped than is successful. In the UK alone, £500 million of card fraud was prevented in the first half of 2024, according to UK Finance's latest data release.

Across the EU, the introduction of strong customer authentication (SCA – see Chapter 3 for more information) has had "a positive impact" on fraud rates, according to the European Central Bank.

This is a battle *we* are winning.

**CNP payments can include:**



Because you and your customer aren't physically together when making a CNP transaction, you're relying on them to provide the necessary details, such as the card number and expiry date.

Not only does this make errors more likely, such as keying in the wrong number when it's being dictated over the phone, it also makes your business more likely to be a victim of fraud.

CNP fraud occurs when a bad actor uses stolen card details to make a purchase. They often appeal to your softer side – for example, spinning a tale about buying in bulk for Christmas, a wedding or making a charitable donation such as toys for an orphanage.

After the items have been supplied to the fraudster, the genuine cardholder files a chargeback request. But by this point, the criminal is long gone – leaving you to repay the cost of the items to the cardholder, as well as the chargeback fee.

A variation of this scam is to arrange for a courier to collect the order, adding a layer of anonymity as no delivery address is given. The outcome remains the same: a chargeback request is raised and your business is left out of pocket.

Brian Kinsella, Senior Regional Fraud Manager at Elavon Europe, says: "We often see that the targets of these frauds are toy shops, electronic stores or bicycle retailers, with the scammer typically ordering that year's 'must have' gift or gadget.

"Interestingly, butchers also face frequent attempts to defraud, often with a sob story, with the caller claiming to have been let down by a supplier for a party and placing a large order for meat at short notice."

Retailers who stock alcohol face a similar threat, with fraudsters claiming supplier problems in the face of an upcoming party before ordering large quantities of alcohol.

But CNP fraud isn't unique to the retail sector, with the hospitality industry also vulnerable.

Hotels can fall foul of **fraudulent pre-paid bookings**, where rooms are booked and paid in advance using compromised card details. These bookings are sold on to unsuspecting travellers who pay directly to the fraudsters.

It results in a financial loss to your business when the genuine cardholder raises a chargeback – and a potential loss in reputation, when the unwitting travellers arrive at your hotel.

Alternatively, in **reservation fraud**, bookings are made on a stolen credit or debit card. This is followed up by a cancellation and refund request, but to a different account. When the genuine owner of the card raises a chargeback, it will be indefensible and the hotel faces a double financial loss.

## Carding

In this type of attack, fraudsters use an ecommerce website to test compromised cards to find details that are valid and active.

Typically, they target a small business' website that has lots of low-value transactions and the fewest hurdles to get over. They then run an automated script, which keeps testing potentially thousands of cards to repeatedly try to secure authorisations.

A successful authorisation, however small, is enough to show the card details work and can be used for more extensive fraud elsewhere.

If details emerge down the line that larger fraud was carried out because of carding on your site, you could find yourself exposed and vulnerable to reputation and legal implications.

On the other end of that extreme, businesses also face additional fees for excessive authorisations and declines from the card brands.

Read more

## Phishing

What started out as glaringly obvious scams – you'll likely have encountered dubious offers of inheritance from a royal benefactor – have now become layered and sophisticated, with even the most astute person left questioning their validity.

In fact, of the UK businesses that suffered a cyber security breach in 2024, 86% had suffered a phishing attack.

The aim of phishing is to lull you into a false sense of security and to catch you with your guard down. It might be a text asking for payment for customs fees, an email from a social media site asking you to click on a link to view a new friend request, or it might be a phone call from a streaming service stating you've paid for an annual subscription to their service.

They're bogus, of course, but cleverly designed to look convincing – resulting in more and more people falling victim.

Sometimes, this type of cybercrime is known as social engineering. You might hear the term 'smishing' for phishing attacks that come by text message – a mash-up of SMS and phishing – and 'vishing', or voice phishing, for over-the-phone scam attempts.

Whatever the method of attack, ultimately the fraudster wants you to respond to the request and provide personal data - typically login details or payment details that can be used to commit fraud elsewhere. With these details, the fraudster can make payments on your credit or debit cards or apply for financial services like loans, bank accounts or cards in your name.

Read more

## Chargeback or ‘friendly fraud’

Chargebacks – not to be confused with a refund – is when a customer questions a payment on their card statement and then claims the money back through the card-issuing bank or card company.

There are legitimate reasons why a customer may raise a chargeback with their card issuer, such as if a cardholder discovers they’re a victim of fraud. But it can be caused by bad actors.

Customers may claim an item never arrived or wasn’t as described on the website or in the catalogue. Alternatively, they may genuinely forget they made a purchase, a mistake often seen with tourists who don’t recognise a charge on their statement because it’s not the expected amount they paid in the local currency.

Then there are the customers who raise a chargeback and return the item, simply because they’ve finished with it. In the retail sector, this is known as ‘wardrobing’ – after customers buy clothes, wear them and then return them – but has spread to other industries including digital-goods suppliers, high-end tech companies and even subscription services.

Not only do you lose out financially from the lost sale, but you also face a fee for the chargeback. And if you incur too many chargebacks, there are further penalties you can face from the card brands.

Read more

## Distraction fraud

Fraudsters try to take advantage of busy shops and restaurants and will try to distract you when a payment is being made.

While the card is being entered into a machine, the scammer cancels the original sale before it’s fully processed and instead issues themselves a refund.

Any business with a card machine can fall victim to this kind of fraud. But if your store, restaurant or hotel is particularly busy, you’re more likely to be a target.

Read more

### There were several high-profile data breaches in 2025.

The UK’s National Cyber Security Centre “urged retailers to be vigilant” after supermarket chains The Co-op and Marks & Spencer, as well as luxury department store Harrods, were targeted in a cyber-attack.

M&S warned the breach could hit the firm’s 2025 profits by about £300 million.

One group has claimed responsibility for the attacks and bragged to the BBC that Co-op “tanked their own sales” by pulling the plug on its own IT systems.

But it has been suggested that the speed with which they acted helped avert a more damaging attack.

These attacks hit sales in the immediate aftermath of the breaches, but it could be years before the full scale of the damage is truly understood.

# Chapter 2:
# Top habits to prevent and detect fraud

You and your team are on the front line of security. Your staff wouldn't let someone walk into your store, pick up stock or equipment and leave without challenging them, at the very least.

That same care and attention should extend to digital and card payment security – whether your business is a bricks-and-mortar location, online only or both.

**This chapter can be summarised with our top five habits to adopt:**

**01**

**Be vigilant, always. If it seems too good to be true, it probably is.**

**02**

**Don't refund to a new account. Ever.**

**03**

**Stay educated. (Guides like this one help.)**

**04**

**Question everything. Train your teams to spot social engineering tactics.**

**05**

**Know your performance indicators. High decline rates in fraud and security or refund spikes? Red flags.**

## Best behaviours to combat online fraud

We always recommend you complete a sense check of orders received, especially with a new customer or for larger amounts than normal. Think:

- **Are you seeing a sudden spike in sales volume?**
  This might be a sign you're being targeted; check back over your recent orders to see if there are patterns to the orders to suggest fraud.
- **Are orders coming in at unusual times?**
  Multiple orders late at night might be a sign this is a fraudster rather than a genuine customer.
- **Are customers buying unusual items (e.g. smart phones or tablets) in bulk?**
  If the buying pattern is unusual compared to your normal sales, this might be a sign of fraud.
- **Are there multiple declines on different cards before the sale goes through?**
  This might be a sign that a fraudster is testing different cards before finding one with sufficient funds available.
- **Does the delivery address match the billing address?**
  If there's a significant difference in the billing and delivery address, it might be a sign that the card does not belong to the customer.
- **Are you seeing multiple orders for the same delivery address but using multiple different cards?**
  Over the course of days, if you're seeing a customer using multiple cards, this again might be a sign of a concerted fraud attack.
- **If it's an international sale, could the customer make this purchase closer to home for cheaper?**
  While ecommerce opens up a world of possibilities, the cost of shipping means that unless your product is unique, the customer is likely to be able to find it cheaper (and get hold of it quicker) if they order close to home.

## Best behaviours to combat in-person fraud

### Protect your terminals

Outright physical theft is one of the more common security issues facing bricks-and-mortar stores, but that doesn't mean you should let your guard down.

- **Keep your card terminals in a safe place.**
  Make sure members of the public can't help themselves to a refund or steal the device. If you have several, regularly count them to ensure none are missing – and contact your provider if any are.
- **When it's busy, make sure staff are aware of where the terminals are and that they aren't distracted when using one.**
  Fraudsters will try to take advantage of a busy location, distracting staff during payment. While the card is being entered into a machine, the scammer cancels the original sale before it's fully processed and instead issues themselves a refund.
- **Set up a password on your terminals for refunds.**
  Then make sure only key staff members have access to it to help prevent unauthorised refunds.
- **Beware of attempts to install card skimming technology.**
  Although usually associated with ATMs, you should regularly inspect your terminals for evidence of tampering. Also be wary of anyone impersonating your terminal provider or vendor.

### Avoid distractions

- **Be wary of attempts to distract your staff and double check the final receipt once it has been printed.**
  If you spot that a fraudulent refund has been processed, contact your payment provider to find out how to void that transaction.
- **Any business with a card machine can fall victim to this kind of fraud.**
  But, if your store is particularly busy, you're more likely to be a target.
- **Be wary of customers trying to play on your emotions and ordering items in bulk – for example:**
  For charity, Christmas presents or a last-minute cancelled wedding. If possible, get them to come in and pay in-person rather than over the phone.
- **And always, always refund to the same card that was used to pay the original sum.**

### What to look out for

- New customers looking to purchase large orders over the phone
- Customers looking for goods to be delivered ASAP – they might even organise a courier themselves
- Buyers who are not too concerned about price, availability or the specific details of the products ordered
- They offer up multiple cards when a transaction is declined

### Three steps to prevent you becoming a victim

- Think through the order. Does it make sense that they are ordering this volume of a product?
- Ask the customer to call into the store and pay by chip and PIN
- Avoid taking payments over the phone (MOTO) where possible; use Pay By Link or Dial Tone Masking instead (see later chapters)

## Don’t forget customer service

Okay, so this won’t necessarily stop bad actors from attempting to steal from you. But it can have an impact on so-called ‘friendly fraud’, chargebacks raised by customers who don’t realise a returns policy, or didn’t receive their product in a timely manner.

Make sure orders are completed in the time you say they will be.

Prevent customers raising costly chargebacks when all they want to do is return their item. Make your returns policy easy to understand.

If you have a lot of overseas customers, make sure they understand what will appear on their card statement. If they are paying in the local currency, explain that the amount on their statement at home could be different because of exchange rates. Or better yet, give them the option of paying in their own currency.

## Best practices for digital security

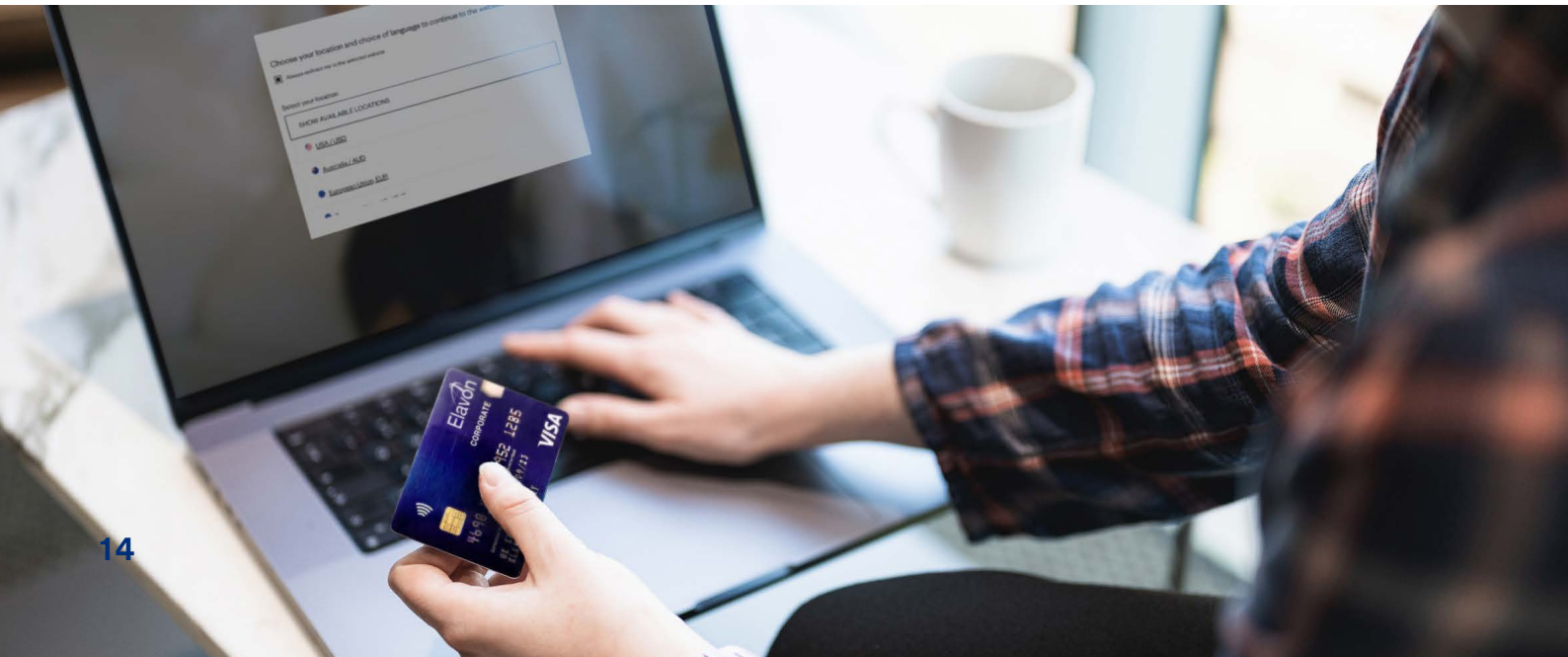
As a small business, payment and physical security aren't your only threats. As mentioned before, almost half of all business in the UK suffered a cyber attack or breach in 2024, according to the UK Department for Science, Innovation and Technology.

The larger the organisation, the more likely they were to be targeted. But more than two fifths of the micro businesses and half of small businesses, were affected according to the government survey.

**Percentage of businesses over time that have identified breaches or attacks in the last 12 months**

| Organisation type | 2025 | 2024 |
|---|---|---|
| Micro businesses | 41% | 47% |
| Small businesses | 50% | 58% |
| Medium businesses | 67% | 70% |
| Large businesses | 74% | 74% |
| Businesses overall | 43% | 50% |

Source: Department for Science, Innovation and Technology



We've already covered what phishing is – often called social engineering – but here we discuss the best ways to prevent falling foul of the practice.

## Be alert

- Is the request coming from a known contact?
- Is this their standard method of communication?
- Are they asking for information that's either unrelated to their query or information they should have themselves?
- Is the email from an official domain linked to the business?
- Is the website the official address for the business or just a similar name?

## Take a moment

When put under pressure, we can sometimes be coerced into carrying out tasks without considering why. Fraudsters will prey on that compliance and try to get as much information as possible by suggesting the issue must be sorted immediately to avoid further impact. By taking a step back to weigh up what's being asked, you'll reduce the risk of being caught out.

## Validate

If you aren't sure if the request you received from a business is legitimate, find the business' contact details online and contact them to see if the request received is genuine.

## Report

If you do fall victim to a scam, then you should report the case to the police who can advise you on what steps to take. However, if you're an Elavon customer and think fraudsters may have obtained information that could compromise your Elavon account, please contact us at fraud.management@elavon.com. We'll support you in securing your account.

You can read more about phishing, what to spot and what to do in the event of a breach on the UK's National Cyber Security Centre website.

# Chapter 3:
# Understanding top security systems

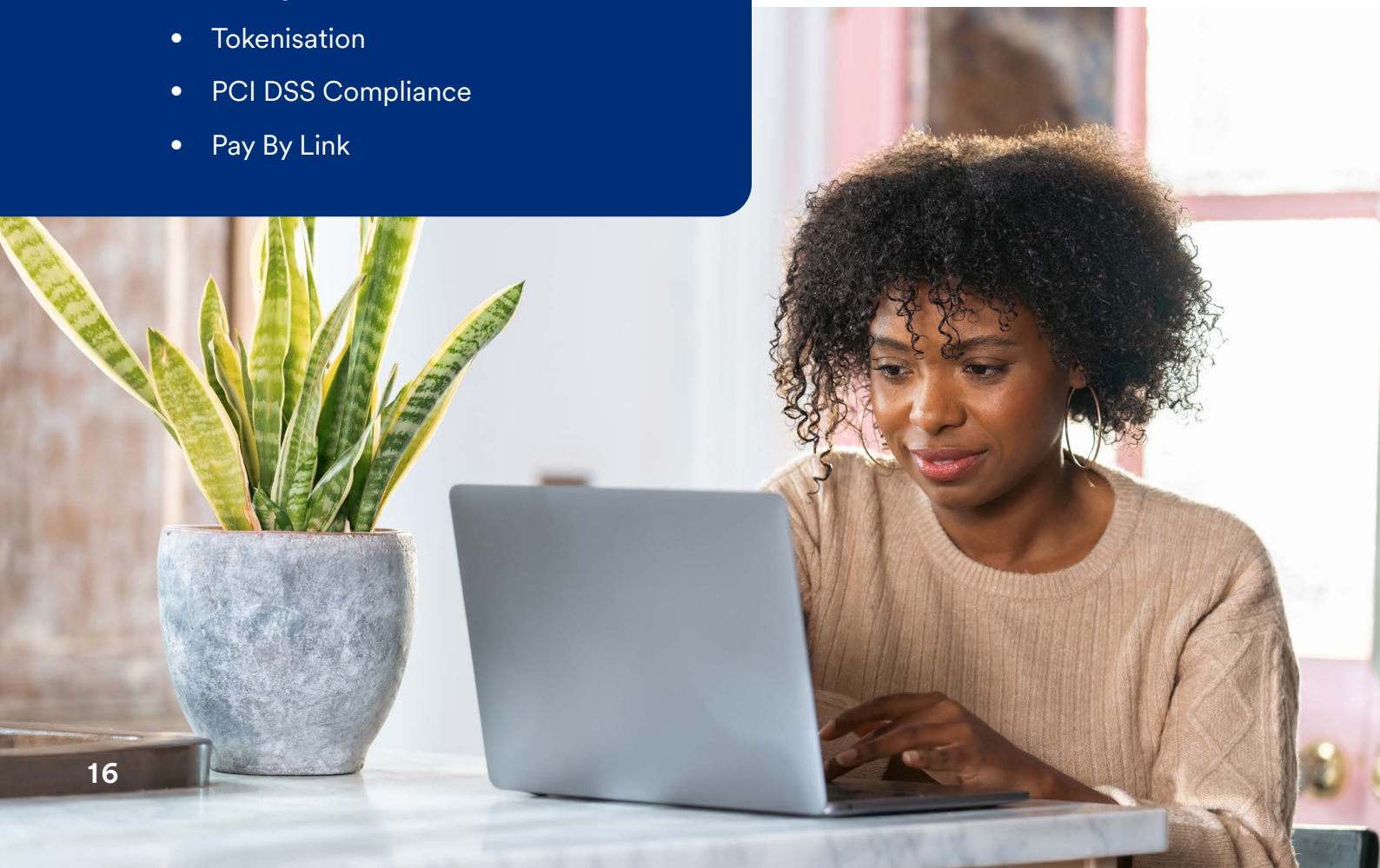
Navigating the wide range of security products available can be time-consuming and requires significant resources.

This chapter will take some of the pain out of that understanding, so you can be better informed about what's available – and what you should consider investing in.

If you think of you and your team as the people manning the ramparts, defending your business from attack, these products are your ramparts. A medieval knight wouldn't go into battle without a suit of armour: you shouldn't face down the fraudsters without protection.

## Coming up, we have;

- Point-to-point encryption (P2PE)
- Strong Customer Authentication (SCA)
- Tokenisation
- PCI DSS Compliance
- Pay By Link



## PCI DSS compliance

Number one on our list is compliance with the Payment Card Industry Data Security Standard. That's PCI DSS compliance for short.

The Payment Card Industry Security Standard Council is a global industry body that sets payments standards that must be met if you want to trade. There are different standards for different organisations, but as a merchant you need to meet the PCI DSS requirements. Not only that, but you also need to prove you've met the standard.

If you're already set up taking card payments, you'll already be aware of the PCI DSS. But across the globe, about 50% of businesses don't bother getting compliance. *"It's because they see it as expensive, a waste of time or they haven't taken the effort to learn about it,"* says Candice Pressinger, Director of Customer Data Security at Elavon Europe. *"Instead, they pay a monthly fee to their payments provider and then cross their fingers they'll never be the victim of a data breach.*

*"But being compliant is good for everyone. It isn't just a 'tick-the-box' exercise; it's a way of ensuring you're protected against attack, protecting you and your customers' data. If you do suffer a data breach and you haven't bothered with PCI DSS compliance, you run the risk of fines running into millions."*

### Non-compliance fees

In 2025, non-compliance fees were reintroduced for Level 1 and Level 2 businesses. Effective from 31 May 2025, merchants who have been non-compliant for a period of 13 months are subject to fees. Specifically, Level 2 firms will incur charges of $5,000 per month, while Level 1 companies will face fees of $10,000 per month.

Should these businesses remain non-compliant after an additional year, the fees will increase to $10,000 per month for Level 2 firms and $25,000 per month for Level 1 companies.

Achieving PCI DSS compliance has always been considered best practice for maintaining the ongoing safety of business and customer data. However, non-compliance now carries significant financial implications. These costs are in addition to the potential expenses associated with data breaches, which can amount to hundreds of millions. These fees are always issued in US dollars.

So how do you get compliant? We have a separate guide if you need detailed help with that, but you can also speak to your payment provider to see if they can offer assistance. If you're already with Elavon, there are three levels of support available:

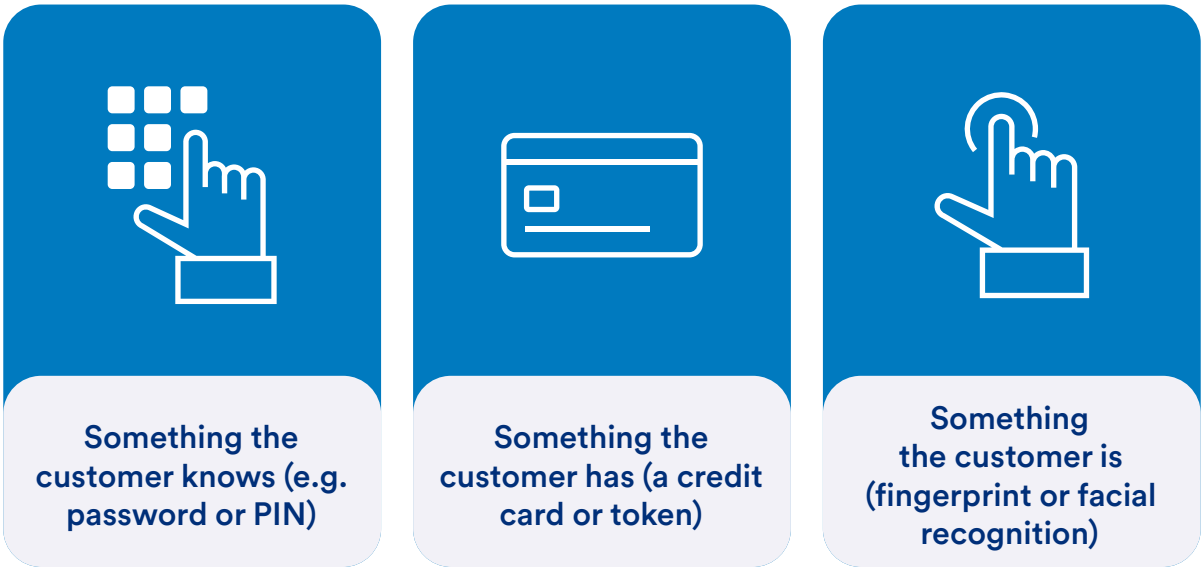
- **Do it yourself**
- **Do it together**
- **Leave it to us**

Even if you opt for the 'do it yourself' option, you still get support from a qualified security assessor and you'll be enrolled in the PCI Fee Waiver Protection programme, meaning if the worst does happen, you'll get cover up to £60,000 or €60,000 depending on where you trade.

## Strong Customer Authentication

Like PCI DSS, if you take payments, you should already be aware of SCA. It was part of regulation introduced under the second Payment Services Directive (PSD2) by the EU and fraud rates dropped rapidly because of the systems it put in place.

So, what is it? Customers must meet two of the following three criteria to be authenticated.




For in-person payments, that's relatively simple. Your customer **has** a credit or debit card and they **know** the PIN. But what about online? Biometrics really help with digital wallets, such as on a phone. For the transaction, the customer **has** a token (see below for more) and **is** who they say they are, verifiable through their unique facial features.

But if payment is taken on a browser, that's not so simple. That's what 3-D Secure is for. This is where a customer is redirected from your website to their bank's site, to prove they are the cardholder at the point of payment. You have to have 3-DS on your ecommerce site if you're based in the UK or EU.

But remember: not all online sales fall under the PSD2 regulation – for example, if you have international customers from outside the European Economic Area (EEA) or the UK. A joint report from the European Central Bank and the European Banking Authority, found that fraud rates for payments involving a card holder outside of Europe were ten times higher than for someone within the EEA.

You can still ask your gateway provider to activate 3-DS for all purchases. If you still want to keep it as optional, make sure you understand which transactions have been processed as 3-DS and which have not.

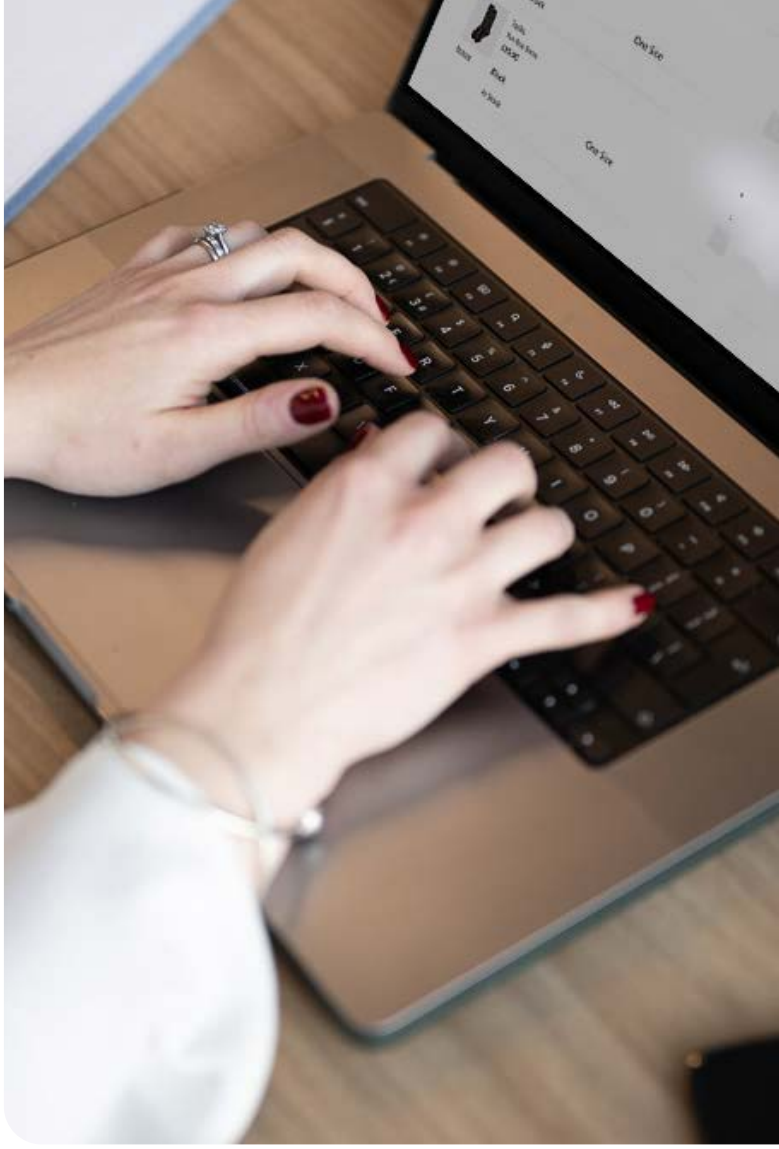

1 2 3
4 5 6
7 8 9
0
Elavon

## Point-to-point encryption

Many of us will be familiar with the word encryption from the use of popular messaging apps. A piece of code scrambles your message, which can then only be unscrambled by the intended recipient of the message. That way, if anyone intercepts your message before it reaches its location, it is unreadable.

Point-to-point encryption (P2PE) is the same thing, but for card payments. It requires a card reader, known as a point-of-sale (POS) device or point of interaction, which has P2PE software built in. All applications on the POS device must also meet P2PE standards.

For ecommerce sales, the encryption is built into the gateway. That way, when a customer on your website enters their card details, it's all immediately scrambled and can only be unpicked by their bank.



## Picture this...

Al Smith goes to his local newsagents to buy a magazine, a litre of milk and a lottery scratchcard. When asked for payment, he places his card into a reader, enters his PIN and hits the green button.

Software on the reader turns all the relevant data to do with the transaction into a string of apparently meaningless numbers.

This is transmitted to Al's bank, which has a secure key to allow the data to be unscrambled. The bank can then do its business, namely confirm Al is the cardholder and has enough funds in his account. This information is returned to the device in the newsagents, and the transaction can be authorised. Al goes home, happy with his purchase.

If the worst was to happen, and hackers managed to intercept the request somewhere between the newsagent and the bank, all they would have is the string of meaningless numbers.

Al's personal data would be safe – and the newsagent avoids huge fines and business-ending damage to its reputation.

The benefit of point-to-point encryption is not just the protection of data, but it makes PCI compliance a whole lot simpler.

It's a win-win: you save time with your PCI compliance form and you're much less likely to suffer a damaging data breach. On top of that, in the unlikely event of you becoming a victim of fraud, having had point-to-point encryption installed, and with your PCI compliance up to date, the authorities will look very favourably on you.

## Tokenisation

Tokenisation sits hand-in-hand with encryption. Like point-to-point encryption, the sensitive data is replaced with a unique set of numbers, known as a token.

The token service, such as your payment services provider, stores the original sensitive data on behalf of the merchant and gives the merchant a token. This token is then used in place of the sensitive data when authorising a payment.

Where P2PE needs code at both ends of the process to understand the scrambled information, tokenisation creates a new piece of data unique to that ecosystem. The token allows transactions to take place, but only between that cardholder and that merchant.

Tokenisation gives you and your customer a double win. From a security point of view, tokenisation means you're not handling sensitive data. The information you do handle would be next-to useless to any fraudster who got their hands on it.

But it also provides a frictionless, pain-free way of paying for things. Your customer can be confident their data is secure, without any impact on the level of service. It's particularly useful for recurring payments, such as subscription payments, or for customers returning to your online store.

Either way, it eases the payment process while increasing security. Win-win.

There's also another form of tokenisation called network tokenisation. This works in much the same way – replacing sensitive PAN data with a meaningless string of numbers – but the token is stored by the card networks, such as Visa and Mastercard.

As well as providing the added layer of security, this form of tokenisation means when the cardholders' card details change – when a replacement card is sent out for example – the token remains the same. No more missed gym payments!

## Pay By Link and Virtual Terminals

These two products are perfect examples of optimisation first, rather than security but they are a way of increasing security.

Pay By Link is a way of taking online payments without the need for your business to establish and run an ecommerce website. Instead, you can email or text the link to a customer which directs them to the payment provider's website. Everything is hosted on your behalf, saving you the need – and associated stress and fraud issues – with building a website.

It's particularly useful for businesses that have been taking payments over the phone. Often known as MOTO payments (mail order/telephone order), these card-not-present payments are often considered some of the riskiest. Because the fraud rates for MOTO transactions tend to be higher, the associated costs are also higher.

By using Pay By Link instead of MOTO, you're both increasing the choice of payment options for your customers and increasing your security.

There are always cases when MOTO remains necessary, for example if many of your customers don't have access to the internet. To help mitigate the risks of MOTO, Virtual Terminal can help. This is exactly what it says – a card machine but one that exists in the cloud. The business accesses the terminal through their browser where they enter the customer's details.

It helps reduce fraud risks for MOTO payments by removing the need to store card details, while also giving access to ecommerce fraud tools such as address checks. Virtual Terminal and Pay By Link will both help in the fight against fraud, while giving your customers more options to pay the way they prefer.

If you need to take lots of card payments over the phone, from a call centre for example, you might want to consider dial tone masking functionality. This allows customers to enter their card details by pressing the numbers on their telephone. The masking means the call handler can't tell what numbers are being pressed, and the payment details are transferred more securely.

### The benefits of more than one defence

*"The best defence is what we call a layered approach,"* says Candice. *"Think of each security system as a brick in your defensive wall. The more bricks, the harder it is for the criminals to breach.*

*"You know your business better than anyone, so you know what security systems will work best for you. And the better informed you are, the better the decisions you will make."*

# Chapter 4:
# The future of security

So, what next? As a small or medium-sized business, you need to consider what happens in the future – both as you grow and as security threats change and adapt.

Not all security products are suitable for all businesses. Like children, as your business grows you might find the problems are less frequent, but get bigger.

Keeping one eye on the future is always wise. That's why at Elavon we pride ourselves on being able to grow with our customers. From the smallest start-up entrepreneur selling pretzels out of a van, to some of the largest airlines in the world – we can help them scale-up to protect their data.

## Artificial Intelligence

Generative AI is the hot topic. From Hollywood blockbusters to the tiniest marketing campaign, major pharmaceutical breakthroughs to personal accounting, everything is going to change in the coming years.

Despite its relative infancy, AI is already being used by criminals intent on stealing data, information or just generally cause a nuisance.

In 2024, British multi-national engineering firm Arup admitted it had been the victim of fraud.

An employee in Hong Kong was tricked into sending $25 million to criminals after encountering a series of sophisticated faked videos of the company's chief financial officer.

The layered fraud, which involved video conference calls, was created using AI technology.

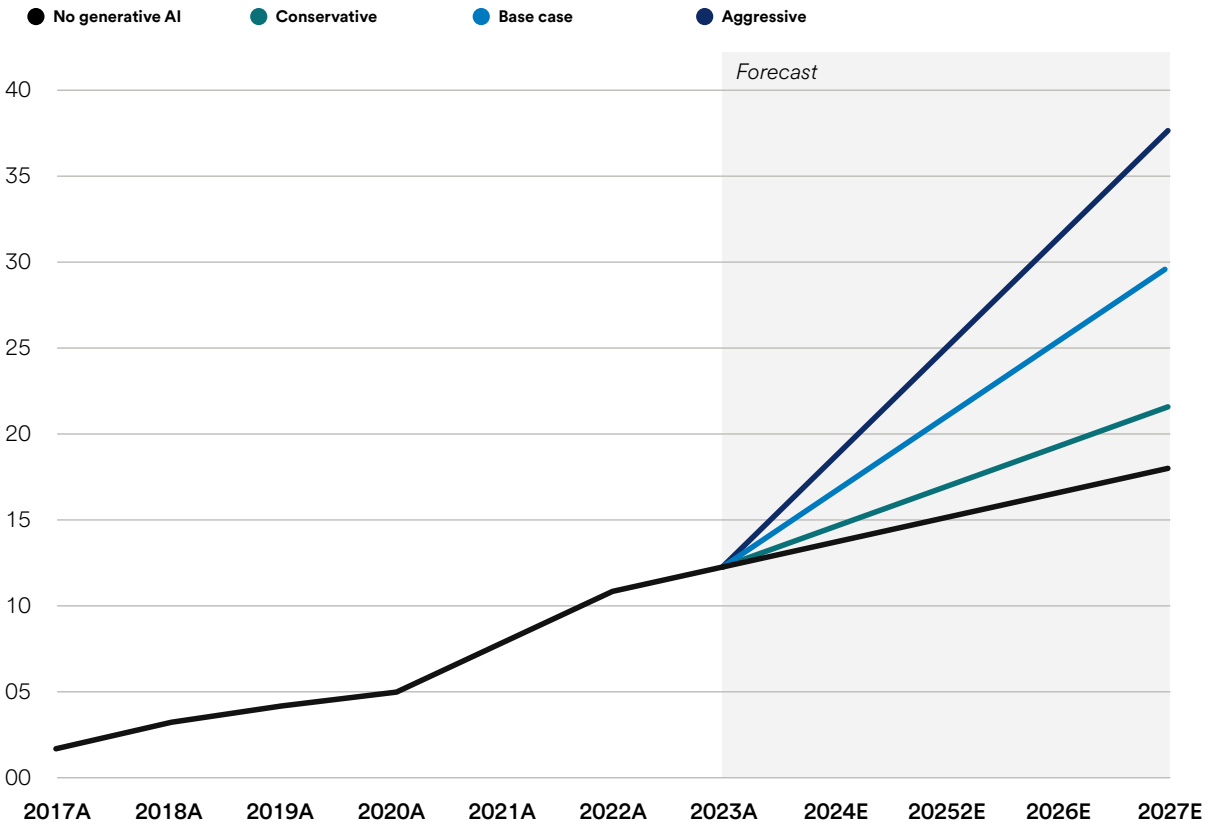
The most well-known generative AI programme only launched in 2022, but the technology is now being used to steal millions of pounds a year.

Consultancy firm Deloitte estimates generative AI could contribute to fraud losses which in the US alone could rise to $40 billion a year by 2027.

*Figure 1*

**Generative AI is expected to rapidly increase fraud losses in the years ahead**

Fraud losses, actual and expected, 2017 to 2027 ($US billion)




Sources: The FBI's Internet Crime Complaint Centre; Deloitte Center for Financial Services

**deliotte.com/isights**

Meanwhile in the UK, the National Cyber Security Centre believes AI will "almost certainly increase the volume and heighten the impact of cyber attacks" in the coming years, with particular focus on social engineering, such as phishing.

And the Alan Turing Institute said the concerns about AI-enabled crime are so high, the UK should establish an AI Crime Taskforce.

## But it's not all bad news.

Artificial intelligence has the power to transform payment security. AI systems can analyse massive volumes of transaction data in real time, identifying anomalous patterns quickly. Much faster than any human can.

*"The key will be to adopt adaptive, AI-driven defences across the whole customer journey before fraud techniques fully emerge,"* says Candice.

*"Talk to your payment provider to understand what AI products are available and suitable. If you're taking lots of small online payments, you might want to consider something like Transaction Risk Analysis [see below]. Or perhaps you want to integrate a machine-learning fraud prevention tool via your website, a solution that analyses transactions in real time and flags suspicious activity before it can do damage".*

*"Not every solution is suitable for every business, but you need to know what's out there to build an effective defence."*

## Biometrics

Biometric authentication has already helped smooth payment processes, especially in light of PSD2.

As part of that piece of EU regulation, it's easy to prove the **'something you have'** requirement with a fingerprint or facial recognition if you're paying with a digital wallet, like on your phone.

Think how easy it is to pay in-app by double clicking a button on the side of your phone, with your face doing the rest of the security work.

Meanwhile, in homes across the world, voice-activated technology is not uncommon. Its use in the hospitality industry is already a reality.

Further improvements in technology could see other characteristics and traits, unique to every individual, used as part of biometric authentication.

People's behaviours – such as the way they hold their phone, type on the keyboard or move their mouse across the screen – could be used as an identifier

*"These really exciting developments will help build a better picture of an individual, so you can be more confident you know your customer is who they say they are,"* says Candice.

*"It has the potential for security measures to be built-in across the whole customer journey, rather than saving it up for the checkout."*

And you'll be pleased to hear that more than two thirds of consumers across the world are interested in using biometrics to identify themselves when paying online, according to Discover Global Network's Global Payments Survey.

## Transaction risk analysis

**What else is available to you, right now?**

While the introduction of Strong Customer Authentication has hugely reduced fraud rates, it has added a layer of friction to the checkout process for your customer.

If you're taking lots of low-risk transactions online, you might want to consider introducing transaction risk analysis (TRA).

Here, the TRA analyses the risk of transactions. If it considers the purchase to be of low enough risk, it requests an exemption from SCA. It means the customer won't be challenged to authenticate themselves using 3-DS when checking out.

You can learn more about TRA, including our award-winning version of it, on our website.

## What's coming next?

As your business grows and the fraud landscape shifts, it's not just about staying safe it's about staying smart.

We're seeing threats become more sophisticated, more targeted, and unfortunately, more effective. But the good news? The tools to fight back are evolving just as quickly and they're becoming more accessible for businesses of all sizes.

### Smarter AI, earlier in the journey

Fraud doesn't start at the checkout anymore — it can begin the moment someone lands on your website. That's why the future lies in real-time, AI-driven tools that can spot risk signals early and adapt instantly. Remember we said biometrics would use more than just your face at the point of check out? That they would spot behavioural habits as you browsed a website?

Well why can't fraud defences do something similar? Unusual behaviour can be picked up at any point in the customer journey. Not only that, a defence that learns on the job.

### Exemptions with AI for Dynamic routing

Strong Customer Authentication (SCA) was a good step, but let's face it too much friction kills conversion. Tools like Transaction Risk Analysis (TRA) are already helping merchants reduce unnecessary challenges. The next step? Smarter exemption orchestration getting security and a smooth experience, every time.

### Security that's built-in, not bolted on

The future of fraud prevention is end-to-end. It's integrated, adaptive, and invisible. That means less firefighting, more optimisation and higher approval rates without compromising safety.

*"We can't rely on black box systems we don't understand. What's coming next is explainable AI tools that show you why decisions are made, and let you adjust the controls,"* says Candice.

*"You don't have to be a data scientist to make smart calls on fraud."*

## Future-proofing checklist: Five moves for smarter security

**01**

Talk AI – Ask your provider what AI-based tools can be activated in your checkout journey.

**02**

Embrace Biometrics – Explore biometric options to streamline authentication and boost conversion.

**03**

Enable TRA – If you process lots of low-risk payments, talk about applying SCA exemptions with transaction risk analysis.

**04**

Layer Up – Use a mix of tools, tokenisation, PCI compliance, 3DS, P2PE to stay one step ahead.

**05**

Stay Informed – Cybersecurity is moving fast. Commit to reviewing your approach every 6–12 months.

# Chapter 5:
# What to do in the event of a data breach

## How to respond when cardholder data is possibly compromised without losing control

You don't get a second chance to handle a data breach well. In the chaos of an incident, your preparation, speed, and discipline are everything. This isn't just about computers, it's about business continuity, customer trust, and regulatory survival.

Here's how to lead through the crisis, step by step, fully aligned with PCI DSS v4.0.1 and card scheme expectations.

### Report Immediately – we are not the PCI Police, we are here to help you get through this

If you suspect or confirm that cardholder data has been compromised—don't wait.

Contact your payment provider's security team immediately. At Elavon, that's the Global Client Security Team:

**Email:** ADCqueries-EU@elavon.com

**UK:** 0207 330 2031

**IRE:** 0402 25326

Early notification triggers fast-track support and reduces exposure to scheme penalties.

## Preserve the evidence

This is a live crime scene. The golden rule? Do not access or alter compromised systems. These are our recommended best practices.

| In card-present environments | In card-not-present environments |
| --- | --- |
| Stop processing transactions on the affected terminal | Stop processing transactions on the impacted server |
| Isolate compromised systems from the network by unplugging the network cable. Don't turn the unit off or remove/interrupt the power supply | Remove and disable storage of sensitive authorisation data |
| Disable remote access ports from the network | Disable remote access ports from the network |
| Change passwords used to connect to the network | Change all passwords used to connect or administer the website |
| Process transactions using an alternative method | Process transactions using an alternative method |

These steps support compliance with PCI DSS v4.0.1 Requirement 12.10.5 (preserving evidence) and 12.10.7 (handling unprotected PAN found outside the Cardholder Data Environment).

## Trigger your incident response plan

Activate your organisation's Security Incident Response Plan immediately, as required by the PCI DSS.

**Include all relevant internal and external stakeholders:**

- Executive leadership
- Legal, HR, and PR teams
- IT and security teams
- Payment service providers or web hosts
- Your acquiring bank (Elavon)
- Law enforcement or Data Protection Authorities, if needed

If you don't yet have a tested response plan in place, create one now. The PCI DSS requires documented, role-specific plans that are reviewed annually and supported by staff training and simulation exercises.

## Engage a PCI forensic investigator (PFI)

If cardholder data is or may be at risk, Elavon will advise you and can support you in engaging the appropriate forensic investigation, which may include a PCI-approved Forensic Investigator (PFI), a third-party Acquirer Led Investigation (ALI), or a third-party Micro Assessment. The company chosen to perform a forensic investigation must be separate from your Qualified Security Assessor (QSA) company.

**Deadlines for engagement of a forensic investigation can be strict depending on the nature of the data security event:**

- Day 5 – PFI must be identified
- Day 10 – Contract signed
- Day 15 – Investigation begins

**PFIs will define:**

- How the breach occurred
- What systems were impacted
- What cardholder data was exposed
- Which accounts are "at risk"

PFI findings form the foundation of remediation, reporting, and recovery and can be mandatory under card scheme rules.

## Communication is key

You should communicate with everyone affected, quickly and clearly.

**Ensure the following parties are informed:**

- Customers, business partners, suppliers and other external groups that might be affected
- Internal stakeholders such as executive, legal, risk, communications
- Your acquirer processor and the card schemes (If you're with Elavon, we'll do this with you)
- Local law enforcement (if applicable) and the relevant Data Protection Authority under GDPR (within 72 hours, if personal data is involved)

This supports both PCI DSS and global regulatory requirements including Article 33 of General Data Protection Regulation.

## Assess the exposure

**With your forensic investigator and acquirer, determine:**

- Was Primary Account Number (PAN), cardholder name, expiration date or service code accessed?
- Was it encrypted or plaintext?
- Was Sensitive Authentication Data (e.g. Card Verification Code, full track data or PINs) stored in violation of PCI DSS?

Understanding your data footprint determines possible liability and your path to resolution.

## Control the fallout

**Beyond the breach comes the clean-up and you'll need to start rebuilding your systems and trust. You might need to anticipate:**

- Increased PCI compliance validation requirements post-breach
- Possible engagement with a Qualified Security Assessor (QSA)
- Potential card scheme fines
- Potential GDPR fines (up to 4% of global turnover)
- Reputational damage and customer attrition

Mitigation is possible but only if you've followed the right steps from the start. You should communicate continuously with everyone affected. Use plain language facts about the breach and what people can do to protect themselves.

## Strengthen. Don't stall.

**A breach is probably your lowest point as a business. But use it as a turning point and reset your defences.**

- Patch vulnerabilities identified in the forensic investigation report
- Revalidate PCI DSS compliance post-breach
- Review third-party access and segmentation controls
- Improve logging, detection, and alerting (Requirement 10)

And don't forget: under PCI DSS v4.0.1 Requirement 12.10.7, you must have a specific process for handling card data found outside your defined secure environment. This is not optional it's the new standard.

## Conclusion

*"The breach is not the end. It's your proving ground,"* says Candice. *"With the right response, you can emerge stronger, sharper, and more resilient.*

*"It's not a matter of when you come under attack, it's if. As we've already explored, almost half of all SMBs suffered a cyber-attack in 2024.*

*"You need to be prepared to prevent the worse from happening. If and when that does happen, we will be by your side, from detection to remediation - you won't face it alone."*


£823k

# **Glossary:**
# The Elavon jargon buster

If there's one thing our industry's good at, it's baffling people with jargon. So we thought we'd give you a cut out and keep translation of some of the main offenders.

**You're very welcome.**

**3D Secure (3DS)** – when paying online, sometimes customers get redirected to their bank for extra checks. Those are 3DS checks.

**Acquirer** – that's us! An acquirer is the business that moves money from your customer's bank to your merchant bank. For instance, when someone buys food in a shop, we take the money from their bank and give it to the shop (after a few security checks).

**API (application programming interface)** – a bit of programming that allows two or more pieces of software to talk to each other. We use them so you can use our services on your website or with your software.

**Authorisation** – when paying with a card and it all goes through, it's been 'authorised'.

**Authorisation fees** – when someone pays by card, a request gets sent to their card issuer (see card issuer) by the payment processor to check the transaction and authorise it. They send a code back to the till so the payment can go through. It all costs money for the payment processor, and that gets passed on to you, the merchant, as a fee. You might see it shortened to 'auth fees'. See also acquirer

**Batch and batching** – the way lots of different payments get grouped together to make it easier to process and settle those payments. So, a restaurant might combine all the payments they take each day and submit the combined batch to us rather than sending us each, individual payment.

**BNPL** – buy now, pay later. It's when someone agrees to pay for something over a few months or years rather than in one big go. You see it more and more these days towards the end of the process when you're buying online.

**Card Present (CP) and Card Not Present (CNP)** – when paying for something over the phone, email or through mail order, it's known as a 'Card Not Present' purchase. Buying online is often classed as ecommerce. And everything else is 'Card Present'. See also MOTO below.

**Card issuer** – this is the organisation that gives (or issues) debit or credit cards to cardholders. It's often, but not always, a bank which manages the account. An example would be your current account debit card. Most card issuers are not card schemes, but some card schemes work as card issuers as well. See also card schemes.

**Card scheme or card brand** – these are the companies that provide the payment networks allowing for card payments. The most common are Visa and Mastercard, but you'll also see American Express, Discover, JCB and China UnionPay. They also set the rules to keep the system running and safe.

**Chargeback** – not to be confused with a refund. If someone questions a payment on their card statement and then claims the money bank through the card-issuing bank or credit card company, that's known as raising a 'chargeback'. It's often because they suspect fraud which will then trigger an investigation into whether it really was fraudulent and, if so, who should pay back the money as well as any fines. A refund is between you and your customer but, because it leaves you out of pocket, the two terms are often mixed up.

**Digital boarding** – 'boarding' or 'onboarding' is just what some businesses call welcoming a new customer on board. (We prefer to call it... welcoming a new customer on board.) Sometimes the process happens entirely online, which is known as digital boarding.

**Dynamic Currency Conversion (DCC)** – when paying for something abroad and the card machine asks if the customer wants to pay in their home currency or the local one.

**ecommerce** – when buying or selling online.

**Encryption** – when information is protected by a complex mathematical formula. You might have seen it mentioned on a well-known messaging platform. In the payments world, we turn all your cardholder information into code to keep it safe for as long as we're using it. It is 'encrypted'.

**ePOS** – see point of sale.

**Faster Payments** – a piece of software that lets you take payments in real time, so you can improve your cash flow.

**Fixed terminal** – a card machine that's in a fixed location, like a restaurant or shop counter. This is where cards are swiped/inserted/tapped or your phones and watches for Apple or Google Pay.

**Funding batch** – a group of all the credit and debit card payments you take in (usually) a day. We go through the batch and make sure all the money goes to your bank.

**Funding event** – when money moves from the customer's bank account to yours or vice versa, with us in the middle checking and moving the funds.

**Gateway** – a clever bit of software that sits on your website and lets you take online payments.

**Integration** – linking a merchant's payment system and our processing platform.

**ISO** – Independent Sales Organisation. This is a go-between for us and some of our customers, promoting what we do and sometimes giving them extra help with things like customer support.

**ISV** – Independent Software Vendor. Like an ISO but where they sell software. It might be a table booking programme for a restaurant which includes our payment services.

**Merchant** – that's you! Someone or something who sells goods or services.

**Mail order/telephone orders** – sometimes abbreviated to MOTO. When you take payment details over the phone or by mail rather than in person or online.

**Multi-currency conversion** – lets you take payments in different currencies, from customers using a foreign payment card. It means easier spending for the customer and more sales for you.

**Omnicommerce** – when the same person or business sells goods or services online and in a physical shop.

**Outsource TRA** – a service we offer, where a merchant tells us which payments don't need TRA, and we then send that information to the issuer.

**P2PE** – point to point encryption. When a card or mobile device is used to pay for something, the data is encrypted and passed to us. From there, we decrypt and process the payment. It makes payments safer by stopping anyone else from trying to steal your data while it's being passed from point A to point B.

**Pay by Link** – if your business website doesn't have a conventional way to buy online, we can provide a web link that sends your customer to a payment page instead.

**PCI SSC** – Payment Card Industry Security Standards Council. They set the international standard for security in the payments industry. If you store, process or transmit cardholder data you must meet PCI standards. This is known as being 'PCI-compliant'.

**Point of sale (POS)** – often used as shorthand for a POS device, which is a till. POS is the moment a customer buys something, so the POS device is what's used in that process. Modern POS devices, often called ePOS, can help with stock control, payments, records and much more. They can sometimes take card payments too. See terminal.

**Pre-authorisation** – in the hotel sector, companies 'pre-authorise' payments for things that a guest puts on their room, like food and drink. The amount is approved before anybody knows what it's going to be.

**Reconcile** – when we compare the payments in our system with the ones your business has recorded.

**Strong Customer Authentication (SCA)** – a requirement from the EU that keeps card payments safe when paying online.

**Terminal** – a card machine. Where your customer taps their card, enters a PIN or waves their phone to pay for something. Sometimes it's part of an ePOS system (see POS), sometimes it's a separate machine.

**Tokenisation** – if you want to store a customer's payment information, we can turn the information into a unique set of characters called a token. That way the information's protected against data breaches as you don't keep any actual information.

**Transaction** – when something is paid for.

**Transaction Risk Analysis (TRA)** – a system that detects whether a transaction is low or high risk and, if it's low, exempts the transaction from more scrutiny. It all makes the checkout process a whole lot quicker for you, without exposing you to risk.

**U.S. Bank** – one of the largest banks in the United States and our parent company.

**Virtual terminal** – a feature that lets you take payments securely online. You can use it on any device that's online, instead of needing to use a physical card machine.

**For more information on any of the topics please visit:**

Elavon.co.uk

Elavon.ie