

PROTECT YOUR PAYMENTS

A merchants'
guide to fraud
prevention



INTRODUCTION

This guide is to help businesses who accept card payments defend themselves against fraud.

Debit and credit cards are a fast, convenient and secure way to make and receive payments.

Criminals do however attempt to target businesses, so it is important to take steps to stay safe.



LOOKING AFTER YOUR CARD MACHINE

If you take card payments in person, it's important that the card machine (also known as a point-of-sale terminal) you're using is secure and can be trusted by your customers.

Where to place your card machine

Always **place card machines in secure locations** where you can see them. This helps to stop fraudsters accessing it or removing it from the premises.

Make sure you always know who has the card machine and what they are using it for. If it's a countertop machine, you should be able to securely mount it so that it cannot be moved.

You should never leave a card machine lying around that someone can pick up.

Always **lock away your card machines when they are not in use**. This will ensure that unauthorised transactions are not processed without your knowledge.

Remember to **take regular inventories of your card machines**. If one is missing, you should contact your card payment processor immediately.

Preventing card machine tampering

Criminals sometimes attempt to tamper with card machines to steal card data and PINs. This includes trying to attach a card skimming device to the machine.

Check your card machines regularly to ensure that nothing has been added or attached to them.

Signs that your card machine has been tampered with can include scratches, glue residue, tape or unusual wires. You should also check whether any parts of the machine look a slightly different colour or newer than the rest of it.

Fraudsters may even attempt to place a fake panel over the genuine one, so **check that the keypad is firmly in place**.



Using your card machine securely

Stay alert when you are using your card machine to take a payment.

Fraudsters may attempt to distract you, such as by starting up a conversation or asking questions. This allows them time to alter the transaction amount, use a stolen card, enter a card number manually or issue a refund.

When a customer is using your card machine it's important you **review the screen carefully** when they return it. This helps ensure the transaction has been processed correctly and prevents potential skimming or other fraudulent activities. **Check the receipt after each transaction** so you know the correct amount has been paid in the proper tender.

Keyed-in transactions, indicated by "Keyed" or an asterisk (*) on a receipt, can be a sign of potential fraud if you were not expecting it. Keying in a card number bypasses the security features of chip cards and can indicate that the card information was obtained through skimming or other means.

Keyed-in transactions are the least secure way to take a face-to-face card payment and should generally be avoided whenever possible. If you suspect a transaction has been keyed in without your consent, contact your card payment processor as quickly as possible to seek further advice.

If a card that has been registered as lost or stolen is used to make a purchase, a declined message will be displayed on your card machine. It's possible the customer could be using a card they've already cancelled by mistake, but it's also a sign of a potential fraudster attempting to use a stolen card.

It is important to always **follow the prompts on your card machine**. Deviating from these may expose you to a potential chargeback.

If your card machine prints a 'merchant copy' receipt with a card number on it, you must keep it secure. You will need to make sure you **lock away all receipts** and keep them somewhere safe.



Limiting access to authorised staff only

Only staff who need to use the card machine should be given access.

Set up a PIN on your card machine for refunds and ensure only the right people have access to it. This will ensure no unauthorised refunds can be processed by a fraudster.

If your machine has a supervisor card, it's also important to keep this safe.

Training your staff

Any staff member that can access or use your card machine should know how to keep your business safe from card fraud.

Staff training is essential and should be carried out on a regular basis to ensure safe practices are being followed.

Maintaining your card machine

It's important that your card machines are regularly maintained and the software is updated.

Always **use trusted providers to service your card machines**. Your card payment provider may offer a support package that includes regular maintenance and updates. They may also provide a troubleshooter guide that could help with any issues.

Your card payment provider will issue updates to the machine's software and firmware. **Check for updates regularly** to ensure that the latest features and security patches are in place.

If there's a problem with your card machine or you think it has been tampered with, contact your card payment provider or manufacturer directly.

LOOKING AFTER ONLINE CARD PAYMENTS

If you take card payments through your website or by a payment link, it is essential you do so safely and securely.

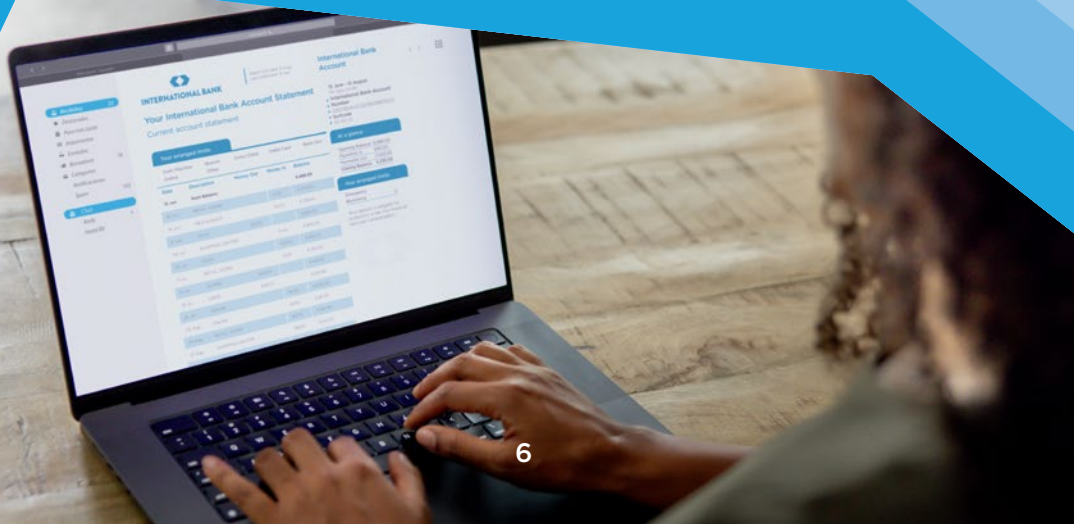
Using a secure payment gateway

A payment gateway connects your business to your card payment processor. Make sure you use a secure payment gateway. Reliable payment gateways with **strong fraud detection and encryption can help you protect data.**

Taking online card payments securely

If you take card payments online, you'll need to comply with what is known as **Strong Customer Authentication (SCA)**, otherwise the payment may be declined. These are rules to make online payments more secure.

Your card payment processor will be able to advise on the security solutions they offer to comply with the SCA rules. This may include **3D Secure** — a security system that helps protect your business from fraudulent payments and the resulting chargeback claims.



When a transaction is successfully authenticated by 3D Secure, any liability to pay a fraud-related chargeback request passes to the cardholder's bank (or similar).

Which 3D Secure system a customer uses will depend on the card scheme associated with the debit or credit card they are using to make the purchase.

Other SCA solutions include those provided by Payment Initiation Services (e.g. through Open Banking), Apple Pay or Google Pay.

For more information about SCA under Second Payment Services Directive (PSD2) visit ukfinance.org.uk



Updating software and plugins

Regularly updating payment software and plugins is important for maintaining security, performance, and compatibility. **Updates will often include security patches that fix vulnerabilities**, prevent potential breaches and protect your data. They may also include new features, improve functionality, and ensure compatibility with other software and systems.

Security certificates and HTTPS

If you take card payments online, keeping **up to date with security standards is essential**.

SSL (Secure Sockets Layer) certificates, also known as digital certificates, create an encrypted connection between a user's browser and your website. This protects sensitive data like personal and payment information from being intercepted by hackers.

TLS (Transport Layer Security) is the newer, more secure version of SSL, though many still refer to these certificates as "SSL".

When your website uses SSL / TLS, your URL will begin with HTTPS. A padlock icon will appear in the browser bar - users can click it to view certificate details, including the issuing authority and your business name.

LOOKING AFTER YOUR CUSTOMERS' CARD DATA

Protecting card data

If your business stores, processes, or transmits card data, **you must comply with the Payment Card Industry Data Security Standard** — also known as PCI DSS. It's a global security requirement to keep cardholder data safe.

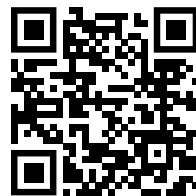
Compliance with PCI DSS is not a one-time task, but an ongoing commitment to secure payment information.

Here are some steps you can take to help safeguard your payments:

- ✓ Don't store sensitive card data, including customer till receipts.
- ✓ Lock away merchant till receipts securely.
- ✓ Use strong, complex passwords for all systems and devices.
- ✓ Install and update antivirus software on all business devices (for example laptops, tablets, mobiles).

Staying PCI compliant helps prevent fraud, builds customer trust and protects your reputation.

For more information about PCI DSS visit pcisecuritystandards.org



Preventing data breaches

A data breach happens when sensitive customer information is accidentally or unlawfully disclosed – often through a security failure. Criminals can use this data to commit fraud.

The most valuable debit and credit card information to fraudsters includes your customers':

- card numbers and expiry dates
- cardholder names and addresses
- card security details like the Card Security Code (CSC).

Don't assume a data breach won't happen to you. Any business that handles card data can be a target. The impact of a breach can be severe – not just financially, but also to your business's reputation and customer trust.

If your business suffers a data breach, you may be required to:

- conduct a forensic investigation to identify the cause
- re-attest your PCI DSS compliance
- pay penalties from card schemes meaning Visa, Mastercard
- report it to the Information Commissioner's Office.

Common breach methods

Criminals use a range of tactics to access sensitive data. Data breaches can often involve human error, so awareness and training are key. Some common methods include:

- **Phishing:** scam emails, messages or websites which trick people into revealing sensitive information.
- **Malware:** malicious software used to gain unauthorised access and steal data. Some malware (known as ransomware) encrypts data and demands payment for its release.
- **Weak or stolen credentials:** attackers often exploit easy-to-guess or reused passwords.

- **System vulnerabilities:** exploiting flaws in software, websites or operating systems.
- **Physical theft:** stolen devices or documents containing sensitive information.

Tips for strengthening your business's digital defences

- ✓ Use strong passwords – don't write down passwords and make sure you change the vendor-supplied default passwords.
- ✓ Use firewalls, up to date antivirus software and intrusion detection systems.
- ✓ Install the latest security patches that are supplied by your vendors.
- ✓ Restrict or limit access to the systems internally.
- ✓ Be vigilant to phishing attacks.



STAYING SAFE FROM FRAUD AND SCAMS

Common scams and how to stay safe

If you have any suspicions during a card payment transaction, it's important to do further checks before you proceed.

There are several things you can look out for when you're taking a payment that could indicate a suspicious transaction. These include if the customer:

- Is unsure of their address or claims they have forgotten some details
- Tries to use multiple cards after one has been declined
- Is making an unusually high amount of transactions
- Is buying unusually large quantities of identical items
- Gives you the right billing address, but then asks for the order to be sent to a different address
- Spells things incorrectly, uses ALL CAPS and what look like fake email addresses.



TO STOP FRAUD™

Take Five to Stop Fraud aims to help you to protect your business by confidently challenging requests for money or information.

STOP: If you receive a request to make an urgent payment, change supplier bank details or provide financial information, take a moment to stop and think.

CHALLENGE: Could it be fake? Verify payments and supplier details directly with the company on a known phone number or in person first.

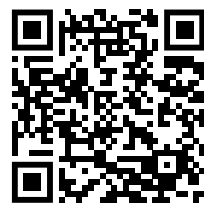
PROTECT: Contact your business's bank immediately if you think you've been scammed.



Top tips to protect your business:

- ✓ Whether it's raising, processing or approving a payment, ensure staff members at every stage of the payment process check invoices and payment details closely.
- ✓ Be wary of unexpected requests for urgent payments – double check the sender's email address and verify the request directly with the colleague or supplier.
- ✓ Always question changes in payment information and confirm details directly with suppliers using the contact information you have on file. Companies rarely change their bank details.
- ✓ Ensure you have robust payment processes and cyber security in place to protect your business and educate employees on these.
- ✓ Be careful with the type of information you share online about your business – criminals can use any information they find to make their scams seem more convincing.

For more information on how to protect your business from fraud visit takefive-stopfraud.org.uk/protect-your-business



Chargeback fraud

A chargeback is when a card payment is disputed by a customer or card issuer which results in the payment being charged back to your account.

Chargeback fraud happens when a customer buys something and then contacts their card issuer to falsely claim a chargeback, for example saying the item was never received.

How to protect your business:

- ✓ Provide clear product descriptions and order status updates, as sometimes chargebacks can be due to customer confusion.
- ✓ Use fraud detection tools and monitor for unusual buying patterns. For more advice on fraud detection tools see our card not present fraud advice.
- ✓ Provide fast customer service to address any issues before they escalate.
- ✓ Work with your courier provider to ensure their delivery procedures are being followed and they can provide you with evidence the goods have been securely delivered to the correct address.



Card testing fraud

Fraudsters sometimes use online shopping websites to test stolen card details to check if they are still valid – a tactic known as carding.

They typically target sites with low-value transactions and minimal security checks, using automated scripts to test thousands of cards in quick succession.

How to protect your business:

- ✓ Implement a bot and spam detection tool, such as CAPTCHA, on your website which helps to distinguish between real users and robots.
- ✓ Use an address verification service at checkout to verify legitimate addresses.
- ✓ Monitor activity on your site, for example by checking the number or speed of payments made within a certain period. Work with your website provider and / or payment gateway to assist with the implementation of tools to stop the testing of cards.

Refund fraud

These scams occur when criminals target a business's card machine to change transactions from sales to refunds.

Criminals may use distraction techniques to draw staff away from the card machine. While the machine is unattended, they quickly issue multiple refunds to their own card. Sometimes they use a different card from the one used in the original sale.

How to protect your business:

- ✓ Ensure card payment card machines are stored in a secure location away from customer access when not in use.
- ✓ Be vigilant of attempts to distract you during the payment process. If you spot any suspicious behaviour, make sure it's reported immediately and keep a hold of any CCTV footage.
- ✓ Ensure card machines are always visible when issuing refunds and are never left solely with the customer.
- ✓ Change card payment machines to PIN access for refunds. The PIN should be changed on a regular basis.

Card not present (CNP) Fraud

Fraudulent card payments made over the phone or internet are known as card not present (CNP) fraud. In these payments you cannot check the physical card details or PIN.

Merchants can be liable for chargebacks, which is why it is important to undertake the necessary checks to confirm that the customer's details and the card are genuine.

Authorisation does not guarantee payment and only confirms that the card has sufficient funds available and has not been reported as lost or stolen at the time of the transaction.

How to protect your business:

- ✓ Ensure you are following the Strong Customer Authentication rules, for example by using 3D Secure authentication (3DS).
- ✓ Look out for unusual orders, particularly for a high value or easily resaleable goods.
- ✓ Obtain the Card Security Code (CSC) which provides additional security digits to confirm that the card number provided is a genuine one.
- ✓ Use fraud screening tools available to you, to help detect suspicious activity. This may include multiple attempts to process a transaction, the same card being used across multiple customer accounts, or the billing and delivery address being far enough apart to cause concern.
- ✓ Fraud detection tools can vary in the level of sophistication they offer. Ensure you are using one that fits your business needs and the settings within the system are customised to suit your specific business.
- ✓ **Taking a payment over the phone is the least secure method for a CNP transaction.** If possible, use a pay by link service as this moves the payment away from a telephone transaction to one that is processed online which can then benefit from 3DS and your fraud screening service.



Courier fraud

Courier fraud is where a criminal uses stolen card details to order goods over the phone and states that they, or a courier / taxi will collect the goods instead of having them delivered.

The fraudster may have the correct name and address details of the genuine cardholder, so things like the Address Verification Service (AVS) check may pass.

How to protect your business:

- ✓ As the goods are being collected there's no way to confirm where they're going. If in doubt, ask the customer to bring their card with them and do the transaction using CHIP and PIN.
- ✓ If an order is being collected by a courier, ask them to deliver only to the specified cardholder address.
- ✓ If someone is placing an order with you for the first time, only agree to deliver to the address registered with the account.



YOUR RESPONSIBILITIES AS A MERCHANT

Understanding merchant responsibilities

As a merchant it is important to **be aware of your legal, contractual and regulatory obligations**.

Card payment processors will continuously monitor for suspicious activity. If a merchant is believed to be acting fraudulently by processing transactions that are not genuine, they will be investigated.

If you fail to meet the requirements set by your card payment processor, they may terminate your agreement and stop providing you with their services. This can be immediate or can take several months to take effect.

Third party processing

Merchants must not allow a third-party to use their card processing account or use another company's merchant account to process their payments.

Using another company's merchant account may breach regulations and contractual agreements with payment processors and card networks.

When a business uses a third-party's merchant account, it has less control over payment processing and may encounter issues with reporting, dispute resolution, fraud and access to funds.

Merchant Category Codes (MCC)

Merchants must ensure they have the correct MCC to avoid issues with payment processing. **Incorrect codes can lead to higher fees or delays in transactions.**

MCCs are four-digit numbers assigned to different types of businesses based on their primary activity.

The codes help determine transaction fees, eligibility for rewards and regulatory compliance.

Regular updates and reviews of MCCs are crucial for compliance and efficiency in payment systems.

Card scheme rules

Merchants must adhere to all rules and procedures set out by the relevant card schemes like Visa and Mastercard.

These rules mandate compliance with standards like PCI DSS, and regulate areas like transaction processing, fraud prevention and dispute resolution.

Merchants who fail to comply with card scheme rules may face fines, fees or other penalties.

For more information visit [visa.co.uk](https://www.visa.co.uk) or [mastercard.co.uk](https://www.mastercard.co.uk)



Legal and Regulatory Requirements

Merchants may face legal action from regulatory bodies or law enforcement if they fail to prevent fraud or are complicit in fraudulent activities.

Merchants could face fines or sanctions for failing to implement adequate fraud prevention measures or prevent money laundering, and for violating data protection and financial transaction regulations.

Relevant bodies include the Financial Conduct Authority (FCA) and the Information Commissioner's Office (ICO) in the UK, as well as the Serious Fraud Office (SFO) who can also prosecute offences related to fraud.

Merchants should establish robust internal controls for detecting and preventing fraudulent activities.

Controls should include:

- ✓ Know Your Customer (KYC): verify customer identity using official documents and for higher risk transactions, conduct enhanced due diligence.
- ✓ Regular audits to identify and address potential fraud risks.
- ✓ Clear reporting mechanisms that allow employees to report suspected fraud confidentially.
- ✓ Regular training to ensure employees are aware of the fraud risks and their responsibilities.



GLOSSARY OF KEY TERMS

3D Secure (or 3DS) is a security protocol that adds an extra authentication step to online card transactions.

Antivirus software defends against malware by detecting and removing malicious software from devices.

Card machine, also known as a card reader or payment terminal, is a device that allows businesses to accept payments from customers using debit or credit cards.

Card payment processor is a financial intermediary that facilitates electronic transactions between a customer's bank and a merchant's bank when a credit or debit card is used.

Card payment providers, also known as a Payment Service Provider (PSP), are companies that enable businesses to accept card payments from customers.

Card schemes allow people and organisations to make card payments by connecting cardholders (those who use the cards) with issuers (the financial institutions that provide the cards).

Card skimming is when a physical device is installed on a merchant's card reader to steal customer card information.

Chargeback, also known as a payment reversal or dispute, is a process where a cardholder's bank reverses a transaction and returns the money to the cardholder.

Firewalls act as a barrier, controlling network traffic and preventing unauthorised access to and from a network.

Merchant is a person or business that sells goods or services.

Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

Payment gateway is a service that facilitates online or in-person payments by securely transmitting payment information between a customer, a merchant, and the payment processor.

USEFUL LINKS

AMEX — americanexpress.com/uk

Citizens Advice — citizensadvice.org.uk

Crimestoppers — crimestoppers-uk.org

Fraud Advisory Panel — fraudadvisorypanel.org

Financial Conduct Authority — fca.org.uk

National Cyber Security Centre — ncsc.gov.uk

PCI Security Standards Council — pcisecuritystandards.org

Information Commissioners Office — ico.org.uk

Visa — visa.co.uk

Mastercard — mastercard.co.uk

Take Five to Stop Fraud — takefive-stopfraud.org.uk

Trading Standards — nationaltradingstandards.uk

Victim Support — victimsupport.org.uk



For more information on keeping your business safe from fraud, visit:



takefive-stopfraud.org.uk/protect-your-payments

Version 1.0, November 2025

