BACS payment fraud prevention playbook

Essential strategies for SMEs

INTERBACS
RELIABLE DIRECT DEBIT PAYMENT SOLUTIONS

According to ActionFraud, payment fraud can be categorised as fraud that involves falsely creating or diverting payments. In 2022 alone, payment fraud losses amounted to over £1.2 billion, the equivalent of over £2,300 every minute.

Despite losses being marginally smaller in recent years, the issue of payment fraud is still a serious threat, with criminals continuing to create more sophisticated methods of obtaining information illegally.

With this in mind, your business must implement effective detection and prevention measures to safeguard yourself and your customers.

In this playbook, we'll cover the different types of payment fraud, ways to detect suspicious activity and, most importantly, how to prevent occurrences of fraud.

Contents

Understanding payment fraud

With the evolution of shopping habits and internet use, criminals are continuously developing and refining ways to commit payment fraud.

Payment fraud can be particularly disruptive for businesses and SMEs. Following an unauthorised transaction, the cardholder will usually raise a dispute. This is where issues begin to arise for your business, as you'll have to take steps to settle the dispute, generally resulting in a loss of time and resources for your business in the form of chargeback and investigation fees.

The first step you can take to protect yourself against payment fraud is through awareness. Let's look at the types of payment fraud which your business could be susceptible to:

Indemnity claim fraud

Indemnity claim fraud occurs when a payer exploits the Direct Debit guarantee by falsely claiming back a payment. In an authentic scenario where a Direct Debit has been taken in error or without authority, the payer is entitled to a full, immediate refund from the bank. This is claimed back through the business that originally took the Direct Debit payment.

When indemnity claim fraud occurs, the fraudster makes attempts to claim back the cost of a Direct Debit through the Direct Debit guarantee, while retaining the goods or services bought. In these situations, a false claim is issued, claiming that the original payment was unauthorised.

If your business hasn't verified the identity of the customer, carried out the appropriate Know Your Customer (KYC) checks or can't provide evidence of sign-up then it's unlikely that you'll be able to challenge the claim, resulting in financial losses for your business.

Strategies for detection:

→ Carry out appropriate KYC checks.

→ Gather evidence of the payer signing up to the product or service

Phishing

Of the 39% of UK businesses that identified a cyber attack in 2022, the most common threat was phishing attempts (83%). Phishing occurs when sensitive information such as login credentials, personal information and card details are obtained unlawfully using deceptive methods such as fake emails, text messages and websites.

These details are then used to make unauthorised transactions and other forms of financial fraud.

Strategies for detection:

- → Encourage employees to adopt safe browsing habits.
- → Educate employees to recognise phishing emails and suspicious email addresses.
- → Keep a close eye on system data and analyse network traffic to easily identify incoming phishing attacks and other suspicious activity.

Spear phishing

Spear phishing is a devious and sophisticated method of phishing where fraudsters target individuals or businesses specifically to trick them into paying credits to the fraudster's account.

Spear phishing is a social engineering tactic which targets individuals and businesses directly. By obtaining as much information about the victim as possible, the fraudster is then able to make contact, often using a spoofed email address, to impersonate a trusted sender. The aim of this method is to extract sensitive information such as log in credentials, banking information or card numbers.

Where regular phishing emails cast a wide net to a large audience, spear phishing is more targeted. These attacks take advantage of familiar information to appear trustworthy to their victims.

Strategies for detection:

- → Conduct email security training for employees.
- → Educate employees to recognise spear phishing emails.
- → Educate employees to recognise suspicious email addresses.

Identity theft

Identity theft is perhaps the most common type of payment fraud. It occurs when an impersonator uses someone else's personal information to make unauthorised purchases, open accounts or commit other fraudulent activities. In 2022, Cifas recorded the highest-ever volume of identity fraud cases in the UK — over 277,000 and a 23% rise since 2021.

Criminals typically target stolen information such as national insurance numbers, bank account details and credit card numbers in this type of fraud.

Strategies for detection:

- → Educate customers on the dangers of identity theft and how to recognise and prevent it.
- → Closely monitor account activities and transactions to identify any suspicious behaviour.

Chargeback fraud

Chargeback, or ‘friendly’ fraud, occurs when a customer purchases using their card and then falsely disputes the transaction with their card issuer, claiming the transaction was unauthorised or the goods weren’t received. If the chargeback is successful, the merchant is liable to return the money to the customer and pay an additional chargeback fee.

This method is used to obtain a refund while also retaining the original product or service purchased. Sometimes, the fraudster will also push for a replacement product and sell the original.

Strategies for detection:

- → Monitor chargebacks to check for patterns of suspicious behaviour and adapt strategies according to any trends.
- → Maintain detailed logs of transactions, including customer communication.

Card-not-present fraud

Card-not-present (CNP) fraud refers to fraudulent transactions made online or over the phone where the physical card isn't present. These can be difficult to track and prevent due to the lack of physical card verification.

Strategies for detection:

→ Monitor transactions for suspicious behaviour or activity which is atypical for the account.

BIN attacks

In this scenario, a fraudulent actor will generate many card numbers based on the card's BIN. They'll then use these numbers to attempt purchases, hoping some transactions will go through.

Strategies for detection:

→ Be aware of small, repeated transactions made from the same IP address.

→ Monitor instances of high purchase volume. Once a card has been cracked, programmed bots can make a large number of purchases in a short space of time.

→ Look out for a high rate of card authorisation errors which can indicate failed attempts of a fraudster attempting to access sensitive information.

→ Identify Card Verification Value (CVV) errors. Fraudsters often can't obtain this information, so incorrect CVV entries can indicate card testing.

Triangulation fraud

Triangulation fraud is a more complex type of fraud when a fraudulent actor sets up a web store with products listed at unrealistic discounts.

After receiving an order, the fraudster will use the customer's personal and shipping information and a stolen credit card to purchase the item from a different source, retaining the fees originally paid to them.

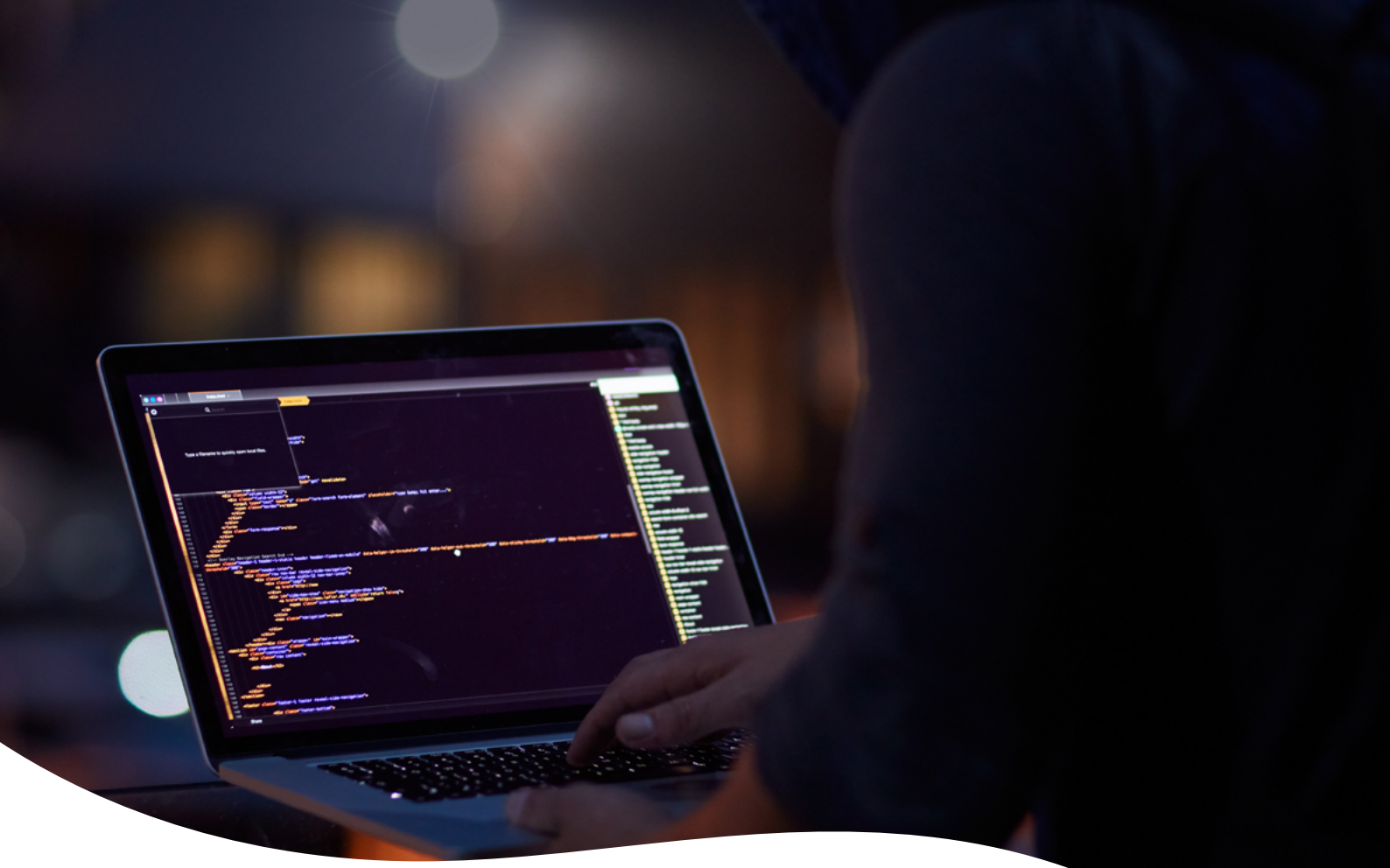
Due to many scam websites being only active for a short period, it's difficult to determine the exact number currently live. However, in 2022, British businesses and citizens reported a suspicious website or email every five seconds, highlighting the rising threat.

Strategies for detection:

→ Recognise fake businesses.

- Check site URLs for HTTPS and a padlock. HTTPS indicates the site's SSL encryption which protects site data from being viewed externally.
- Use a domain-checking tool such as WHOIS to determine the age of the domain. Domains which haven't been active for very long often indicate scams.
- Check for quality. Scam sites often have bad grammar, poor-quality images and a basic website design.
- Investigate missing details. Scam sites usually fail to supply contact details or an authentic returns policy. Checking these details can help separate legitimate sites from scams.
- Check the site's payment options. Scam sites usually try to force users to pay for goods using non-reversible and non-traceable payment methods, e.g. bank transfers, cryptocurrencies or payment apps like PayPal and Cash App.

→ Check suspicious websites for indicators that they aren't legitimate. Identifiers such as spelling errors can be a giveaway.



Account takeover

More commonly known as hacked accounts, this type of fraud occurs when a fraudulent actor logs into an existing customer account and uses their stored information — such as their billing details — to make unauthorised purchases. In some instances, the fraudster will resell the account.

Strategies for detection:

- → Be vigilant and check for unfamiliar changes. Even small changes can be an indication that an account has been compromised.
- → Look for changes to phone numbers and email addresses. These can indicate a fraudster trying to bypass multifactor authentication on an account.
- → Monitor any password reset requests, particularly if they're unrecognised.
- → Check for unusual IP addresses or browsers in your account history.

Overall strategies for payment fraud detection

To effectively combat payment fraud, be thorough and proactive in your approach, ensuring you're well-versed in all areas of payment fraud.

Take time to familiarise yourself with the different types of fraud you may encounter, assess any potential risks and unique vulnerabilities to which your business may be susceptible and implement any necessary detection and prevention measures. Do this in a continuous and evolving way so you can protect your customers' data, maintain financial integrity and safeguard trust in your brand.

Common fraud indicators

You should be aware of several fraud indicators to combat payment fraud effectively. Some of these are easily identifiable, such as false numbers of email addresses, but some may be less obvious. Understanding how fraudsters use information can help protect your business against fraudulent transactions.

Some examples of fraud indicators:

- → Use of false information such as email addresses or phone numbers.
- → Customer detail inconsistencies across multiple purchases.
- → Suspicious-sounding communication which appears to be scripted.
- → Unusually large orders that are inconsistent with normal customer behaviour.
- → Multiple payments are made with the same card but with different shipping addresses.
- → Multiple payments from different cards to the same shipping address.
- → Requests to split a large order into multiple payments, particularly if the buyer intends to use multiple cards with different billing addresses.

Strategies for payment fraud prevention

While detecting and identifying potential threats is important, prevention is the most critical factor in protecting against payment fraud. There are several preventative measures which you can adopt to ensure your business is operating as securely as possible.

Monitoring transactions

During a transaction, monitoring and verifying all important information being processed is vital. Information such as shipping addresses, IP addresses and spending amounts can all offer invaluable insights into the validity of a transaction. Verifying this information can help your business track transactions and reduce the chance of fraud.

Restrict access to sensitive information

Restricting access to sensitive information will reduce the chance of data being leaked or accidentally compromised. By only providing essential employees with confidential information, you reduce fraud risk significantly.

Encrypting data

Encrypting important documents before sending them will ensure the recipient can only view the document and won't be able to alter or manipulate the data in it. By doing this, you can ensure customers can't change important information and use it for nefarious purposes.

Avoid paper invoices

All business transactions recorded on paper are susceptible to theft, leading to payment fraud issues further down the line. To avoid this, you should consider storing such documents electronically.

Use strong authentication

Using a multiple-factor authentication system ensures your business documents and finances are well protected.

Stay updated

With payment fraud methods always evolving, the best way your business can protect itself is by staying ahead of the curve.

Many businesses function primarily online. With this increased connectivity, opportunistic fraudsters are always looking for new ways to obtain and use confidential information. By keeping up to date with current threats, you can take steps to better protect yourself against payment fraud.

Specific strategies for preventing different types of payment fraud

Indemnity claim fraud

- Always complete KYC checks to ensure you can validate any potential customer's details.
- Retain all evidence of customers signing up to a product/service.
- Put controls in place to protect data from both loss and theft.
- Make any necessary counterclaims or challenges if an indemnity claim should arise.

Phishing

- Implement an email filtering system such as DMARC to protect against bogus emails.
- Install firewalls and intrusion detection technologies to protect internal systems.
- Enable multifactor authentication to prevent unauthorised access to important systems.
- Develop a strategy to handle any successful phishing attacks. Strategies can include containment policies, reporting and communication to the relevant departments.
- Verify third-party software to ensure it's secure and won't compromise security measures.

Spear phishing

- Implement email anti-phishing protection which is specifically geared towards detection of spear-phishing.
- Educate employees on checking for domain spoofing, instances of impersonation, and questionable content in emails.
- Keep your systems up to date with the latest security patches.
- Encrypt sensitive company information.
- Use DMARC technology.

Identity theft

- Ensure robust data-security measures, such as encryption, access controls and secure storage, are in place.
- Enable multifactor authentication for accounts.
- Implement customer identity verification, particularly if the customer wants to make account changes or for high-value transactions.

Chargeback fraud

- Enable fraud detection software to recognise suspicious activities for review.
- Use strong verification checks to analyse customer identities and billing information to check for discrepancies.
- Ensure all product descriptions, shipping information and return policies are detailed and clearly defined.
- Nurture customer relations with open and transparent communication to settle any disputes and address any customer concerns.
- Send parcels with tracking to ensure proof of delivery.

Card-not-present fraud

- Implement AVS (address verification service) and CVV (card verification value) for online transactions.
- Implement multifactor authentication for online accounts.
- Comply with PCI DSS (payment card industry data security standard) to protect cardholder data.
- Implement fraud detection tools to identify suspicious transactions.

BIN attacks

- Implement firewalls, time-out detection and CAPTCHA forms as preventive measures.
- Set transaction limits for transaction value or the number of transaction attempts conducted within a set timeframe.
- Conduct verification checks to ensure customers are who they claim to be.

Triangulation fraud

- Check reviews from previous shoppers to establish the seller's authenticity.
- Ensure you have the relevant security credentials so the secure padlock icon appears when customers are on your website.

Account takeover

- Check for compromised credentials. Using a breached credentials database, you can compare user credentials and identify when a user is signing up with known breached credentials.
- Set rate limits on login attempts. Based on parameters such as username, device, and IP address and based on your users' usual behaviour, you can use this method to prevent account takeover.
- Incorporate limits on the use of proxies, VPNs and other factors, which are often used by fraudsters to hide their identities.
- Send account change notifications. By always sending your users a notification of changes made to their account, users can notice immediately if their account is compromised.

But the most effective way to protect your business against payment fraud is to implement reliable software.

About InterPass

Several options are available to small businesses and SMEs when looking for software to protect against payment fraud.

InterPass is a professional identity verification software that enables users to easily and accurately check the identity of potential customers. The software verifies the payee's account name to ensure the validity of bank details. The software can easily identify whether the details are a full match, near match or incorrect, providing exact details of the issue should a check flag as incorrect.

InterPass in use

The process of identity checking can be intricate and complex. However, these complexities can be simplified with the correct software, helping your business concentrate on its day-to-day running while remaining secure.

Interpass allows this, tailoring itself to suit the needs of any business. This off-the-shelf product is mainly tailored to direct debit solutions but can be used for various purposes, from mortgage identity checks to electoral roll identity confirmation.

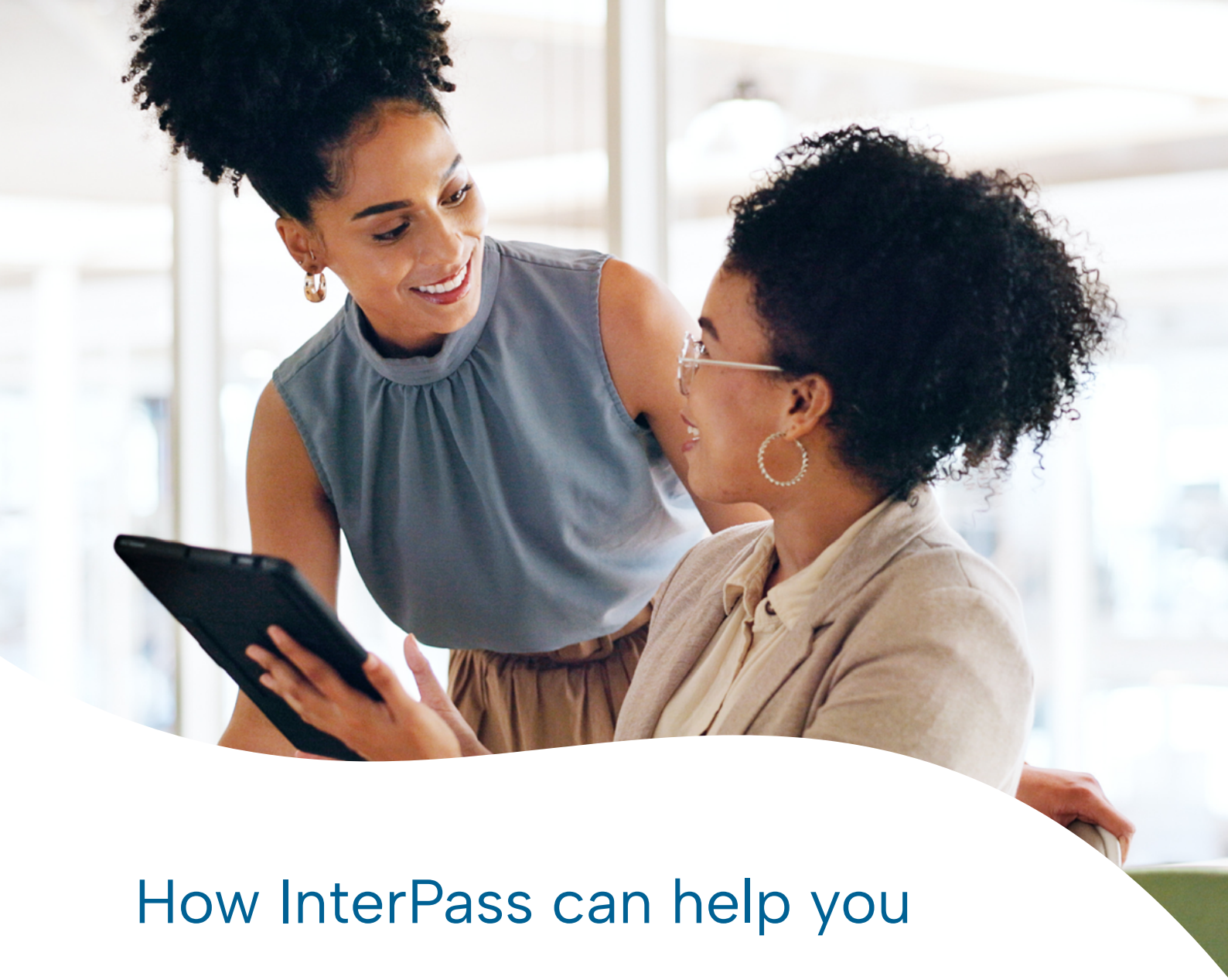
The solution works in unison with other Interbacs products but can also be used independently using the API, meaning it's suitable for various security purposes.

An additional element of InterPass is its ability to perform KYC checks. These checks confirm the identity of customers, reassuring you that your customers are who they claim to be. This helps you stay secure and protects your business from payment fraud.

Equifax & Bacs

InterPass utilises Equifax's service to verify the identity of potential customers. Using this service, InterPass can provide full access to the many tools available from Equifax at a fraction of the cost, catering to the needs of a diverse set of businesses.

InterPass is an intricate identity-checking solution optimised for Direct Debit and payment users. However, the solution is also suitable for other businesses. The API tool allows users to verify the identity of their payers, making it an accessible tool for all types of companies seeking additional security measures against fraud.



How InterPass can help you

For Direct Debit providers offering paperless Direct Debit, InterPass is the ideal solution for fraud protection — the business is responsible for identifying customer identities and validating their details. Interpass facilitates this easily, allowing you to seamlessly integrate the system into your day-to-day processes and perform any necessary validations in the background.

Checking payee details is imperative in fraud detection and prevention. Supplier payments, employee salaries and expenses require vigorous checks to ensure the payee's identity is correct and the funds transfer is secure. Interbacs can perform the initial integration of InterPass, allowing your business to freely use the software to offer you the best protection against fraudulent activity.

It's crucial to remember that failure to verify the payee's identity can result in disastrous consequences, leaving your business susceptible to a loss of funds or payment fraud. Therefore, you must adopt a practical and well-planned approach to tackling fraud.

Get in touch to protect your business from fraud

The rising threat of payment fraud has become a consistent source of concern for businesses, with fraudsters continually evolving their methods and finding new ways to target unsuspecting victims. This troublesome issue can financially and emotionally damage everyone who falls victim.

In this playbook, we've covered the various types of fraud to be aware of. However, combating payment fraud requires awareness and preparation to offer the best chance of protection.

To learn more about the various types of fraud and how to protect yourself, your business and your customers, click below.

Learn more and enquire

INTERBACS
RELIABLE DIRECT DEBIT PAYMENT SOLUTIONS