CREDIT CARD FRAUD

Credit card fraud is the unauthorised use of an individual's credit card. Criminals use various tactics to steal personal information, or even the card itself to make purchases of goods and services. In some cases, criminals can even apply for a credit card in someone's name without them even knowing.

Once opened, they can then apply for loans, purchase items, and apply for more cards. With an estimated 59 million credit cards in the UK, fraudsters see this as a prime opportunity to take advantage of susceptible victims. Here we explore different types of credit card fraud and what to look out for, so you don't get scammed.

Scan to view UK Finance 2024 Annual Fraud Report

CREDIT CARD STATS

Approximately **12.2 million** credit card transactions happen per day*

As of January 2025 almost **59 million** credit cards were in circulation in the UK*

Fraud losses on UK-issued cards (debit, credit and other payment cards) totalled **£551.3M** in 2023**

*finder.com - Credit card statistics.

**UK Finance 2024 Annual Fraud Report.

Lost or stolen cards

The most obvious type of credit card fraud is when a card is lost or stolen. Once the criminal is in possession of a credit card, they will quickly use it for unauthorised transactions until the victim cancels the card.

To reduce damage from this type of fraud, remember to report your card as stolen as soon as possible. This will block any future transactions. For an added layer of security, you can also set up your card to require a PIN to be entered before finalising any purchase.

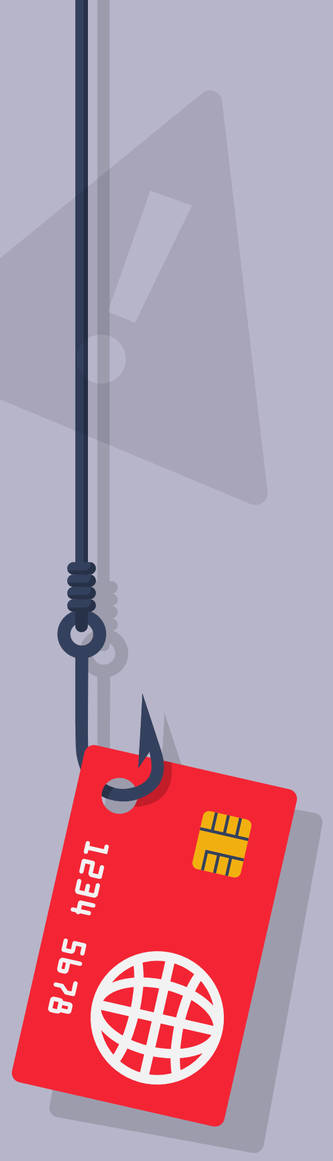
Alternatively, thieves also intercept credit cards sent to cardholders in the mail. Therefore, if you are expecting a credit card and haven't received it within a reasonable timeframe, call your credit card company or bank to investigate.

Phishing attacks and malware

Phishing attacks and malware software can be used to capture personal information which fraudsters can then use in multiple ways. For example, to commit card-not-present (CNP) fraud. This type of fraud is where physical cards aren't needed to complete a transaction e.g. online or over the phone.

Phishing attacks are where criminals send emails or texts to victims pretending to be from a bank or credit card company. This message will often claim that an account or card has been compromised and requires information to secure it e.g. PIN, account/card number, password or personal data. Often panicked and pressurised, the victim will reveal this information to prevent any further danger. Unknowingly, they are providing the scammer with everything they need. Remember that a genuine bank or credit card company will never contact you out of the blue to ask for your PIN, passwords or sensitive information.

Alternatively, fraudsters also use malware to steal account details and passwords. Malware is harmful software that's downloaded onto a device without the victim's knowledge. This software can work in the background completely undetected and can capture credit card information as the victim enters it online, for example when making an online purchase. To protect yourself, use antivirus software and update it regularly. Additionally, avoid clicking on suspicious links and downloading files from untrusted sources. This is how malware can get onto your devices.



Skimming

Having a credit card in your possession is often safe, however be careful, criminals use a tactic called "skimming" which aims to steal your data without you even realising it.

Skimming is a type of fraud that uses a "skimmer" which is a small electronic device, often placed on ATMs, petrol pumps or point of sale card terminals. Skimmers can work in numerous ways:

- A small, inconspicuous device attached on top or inside a card terminal. This device is designed to steal information such as your name, card number and expiry date from the magnetic strip on your card. This takes place when your card enters the machine/terminal.
- A hidden camera or keyboard overlay, designed to capture your PIN information. These are often used at ATMs.

Skimmers can be very hard to detect because they're designed to blend in perfectly with the card terminal or ATM. Once the data is stolen, criminals will use this how they wish. This can include cloning your card to make purchases and withdraw money, or selling the information to a third party.

This type of fraud can take some time for the victim to notice there's a problem. Individuals still have their physical card in their wallet, so they are completely unaware that they have become a victim. Usually, they will not notice until they receive a bank statement.

Signs to look out for:

- Take your time and inspect the card reader. Is it intact? Does it look unusual? Are there any parts which are bulging, unaligned or covered? If so, a skimmer may have been fitted.
- Check for damage on the terminal or ATM which may indicate tampering e.g. scratches, marks, dents, residue.
- Check for hidden cameras.
- Check the keypad. If it feels thicker or higher than usual, or the keys are harder to press, it could be due to an overlay that has been fitted to capture your pin.

Steps you can take to keep yourself safe from skimming:

- Only use ATMs in trusted and safe locations e.g. a bank.
- Using contactless payment methods if you can.
- Always cover your pin when you enter it.
- Monitor your accounts regularly.
- If unsure or something doesn't feel right, either find another way to pay or use another machine. Remember, skimmers can be very hard to detect.

Identity theft

Many different types of credit card fraud involve identity theft. Criminals can use stolen personal information e.g. name, address, birthday and national insurance number in a variety of fraudulent ways:

Application fraud - Criminals can use this personal information to apply for multiple credit cards. The criminal will then make several transactions across these cards which are in the name of the victim. Ultimately, the victim will not be liable for any purchases made, however this type of fraud can harm their credit score. Application fraud can go undetected until the victim applies for a credit card themselves or checks their credit report.

Account takeover - Once scammers have access to the information they need, they contact the credit card company pretending to be the card holder. They then use these details to take over the cardholder's accounts. Passwords, PIN numbers and memorable information will all be changed. Once this has taken place, criminals will then use the account how they wish.

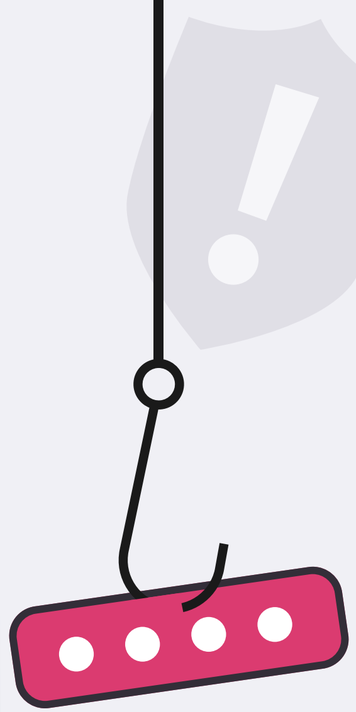
Lost cards - Fraudsters can also take advantage of this information to contact the cardholder's bank and report a lost credit card. The bank will issue a new one, but this time the criminal will ensure it is sent to them. Once in possession, they will go on to make as many unauthorised payments as possible until the victim realises something is wrong with their current credit card.

Remember to be very careful with any personal information you have. For example, do not throw any bank statements in the bin. Make sure you shred these so no information can be stolen.

How to spot card fraud

- You notice any unusual transactions on your bank statement.
- Your credit card is unexpectedly declined when making a payment – if this happens, contact your bank immediately.
- You see something unusual at an ATM or you don't get your card or cash from the machine – criminals can tamper with ATM machines to clone your card. Avoid using the machine and contact your bank immediately if you are impacted.
- You're making a purchase, and the card machine looks different – criminals can tamper with card machines. Avoid using the card machine if you're uncertain.
- You are contacted out of the blue via email, text or phone call from a bank or credit card company asking for account details or personal information.

Advice from Take Five to Stop Fraud



How you can stay safe from credit card fraud

Keep your card safe and shield your PIN whenever you enter it.

If your card is lost or stolen, report it to your bank immediately.

Check your bank statements for unauthorised transactions or suspicious transactions you never made.

Do not give out any personal information if you have been contacted out of the blue via phone, email or texts.

If you have online banking/apps, set up your notifications to come through whenever you make a payment, so you know when it wasn't you.

Make sure only you have access to your post and destroy or shred documents with personal information as soon as you're done with it.

As soon as your card or new card arrives, sign it straight away. If you're disposing of your old card, make sure you cut through the chip and dispose of the sections in separate bin bags.

Advice from Take Five to Stop Fraud

Scan to view Take Five to Stop Fraud website: