Guide to credit card security

Contents

Click on a title below to jump straight to that section.

What is credit card fraud?

Credit card fraud is when someone else uses your credit card details without your consent to withdraw money or make transactions. Your first indication of fraudulent activity may be a call from your credit card provider's fraud team, or transactions you don't recognise appearing on your statement.

Types of credit card fraud

Card-not-present fraud

A card-not-present (CNP) transaction is when you use your credit card over the phone, online or for mail orders. CNP fraud is when someone else makes such transactions without the cardholder's authorisation.

Counterfeit card fraud

Also known as ‘skimming’, this can occur at an ATM or a point of sale terminal. Card details are copied by a skimming device and the PIN captured by e.g. a miniature camera trained on the keypad. A cloned card is then produced and used for fraudulent purposes.

ATM fraud

This is when a fraudster attaches a device to a cash point to trap your card. Fraudsters sometimes also target ATMs to watch as people enter their PIN and then pickpocket the card.

Intercepted mail fraud

A criminal acquires someone else’s credit card or sensitive details sent in the post, then uses the information to commit fraud.

Identity theft

Identity theft involves someone impersonating another individual by using their personal details, often to commit credit card fraud. A fraudulent application for credit could be made under the individual’s name, or a genuine account might be taken over by the fraudster.

Current scams

Courier scam

A fraudster calls you, usually pretending to be from your bank or the police, and tricks you into revealing your PIN and giving your card to a courier.

The fraudster will sometimes encourage potential victims to call the number on their bank card, then keep the line open at their end and pretend to be a call centre agent at the bank. The scammer sends a courier or taxi to pick up the card(s) from your home.

Phishing

Fraudsters attempt to acquire your personal details or bank account numbers by emailing you and pretending to be a genuine person or business. When making purchases online or over the phone, you will never be asked for your PIN.

You may be asked for:

- the long number on the front of the credit card
- the name of the cardholder, exactly as printed on the card
- the card expiry date
- the card security code (CSC) – also known as the card verification code (CVC), or card verification value (CVV) – the last three digits on the signature strip on the back of the card

Bogus text messages

Fraudsters send you a text message, which appears to be from your bank, in order to steal your personal or financial details. These messages often look very authentic. They may claim your bank account has been subject to fraudulent activity and ask you to get in touch urgently, via an illegitimate number or website provided in the text.

Keeping your card and card details safe

It's important to check your credit card activity at least every month and contact your credit card provider immediately if you become aware of any unusual activity. To protect yourself from liability if your card is used fraudulently, you must act with reasonable care whenever you use it. This includes reporting a lost or stolen card straightaway.

PIN number

You will generally authorise credit card transactions using a personal identification number, or PIN. Never write it down or share it with anyone – keeping your PIN secret is essential to ensuring the security of your credit card.

Using your card while out

To prevent your card being used fraudulently, use it with caution and never let it out of your sight.

- When using ATMs or point of sale terminals, be aware of what's going on around you and cover the keypad while entering your pin.
- Avoid using any cash machine that appears to have been tampered with.
- Do not get distracted or accept help from strangers at a cashpoint.
- If your card is retained or stolen at a cashpoint, contact your bank then and there; do not re-enter your PIN.
- When paying a restaurant or bar bill, waiting staff should bring the card reader to you.

Protect sensitive details

- Carefully dispose of sensitive paperwork containing personal or credit card information, such as receipts and credit card statements.
- Never share sensitive financial information online, and keep other personal details to a minimum.
- Don’t email your credit card details (especially not all in the one email) in case the message is intercepted.
- Keep your credit card provider informed of address changes and consider using a mail redirection service for a few months after moving.
- If you notice that a new / replacement card, statement or any other important communication has not arrived, let your card provider know at once.
- Never give your PIN, login details or password to anyone who calls you, even if they say they are calling on behalf of your bank, credit card provider or the police.
- Delete emails or text messages asking for financial details, without responding.
- Do not open attachments from unknown senders or any emails that strike you as suspicious.
- Avoid updating financial details by following links or calling numbers supplied via email or text message.
- Only give your card details over the phone if you have called a company you know to make a transaction.

Banking and shopping securely online

For greater online security, install a firewall and antivirus software on your home computer. Keep these up-to-date and switched on at all times. Never access your online banking account through a link in an email, even if the email appears to be from your bank.

Public networks

Avoid using public wi-fi networks for online shopping and banking, whether you are on a public computer or your own mobile device. Fraudsters have been known to create fake versions of a shop or bar wi-fi network. Then, if you log on to your email or online banking account using the fake network, they can attempt to acquire your login details. It is always safer to access these services at home, or via your mobile phone / tablet data. If you do need to use online banking or make a purchase via a public network, consider the following.

On a public computer:

- Always log out afterwards – it's not enough to close the browser window
- Untick or reject 'remember me' / 'remember password' options
- Try to ensure no one is watching your screen over your shoulder

- Don't leave the computer unattended
- Use the browser incognito setting, or erase your browser history

On your own laptop or mobile device:

- Ask if a cafe or store wi-fi network is genuine
- Consider using a VPN (Virtual Private Network)
- Only use your bank's or a store's official app

Secure websites

When managing your credit card or shopping online:

- Type the URL into the browser rather than clicking on a search engine link
- Check that the URL begins 'https'
- Look for the security symbols – often a locked padlock or key logo:

    - next to the URL in the address bar

    - in the bottom right corner of the browser

Genuine websites

It's not difficult for criminals to clone a website or produce a professional-looking, fake site. Consider the following:

- Genuine websites tend to have a postal address, phone number and / or email
- If in doubt, email or call a company before making an online purchase
- Check if the website URL looks genuine – be wary of:

    - misspellings or extra words

    - characters or numbers

    - URLs that seem unrelated to a business name / trade

- Roll the mouse over links in search engine results to reveal their destination:

    - be cautious if the destination looks different from the link info

Logging in / out

Online banking and shopping login details should be kept private. It's sensible to log out after completing any credit card management or shopping transactions. If you make a purchase, print or save the order confirmation page / email for your records.

Online security systems

Free online security systems, like Verified by VISA, MasterCard SecureCode and American Express SafeKey, add an extra authentication step when checking out, to make online transactions more secure.

Using your card provider's particular online security system could also protect you from liability if your card is used fraudulently.

Payment gateways

You can avoid online traders or sellers seeing your credit card details by using a payment gateway, such as PayPal. This can be especially useful if you're making a purchase from a store or individual you're unfamiliar with.

Be aware that you may not enjoy the same protection under Section 75 of the Consumer Credit Act as you do when paying with a credit card direct.

What to do if your card is lost or stolen

Notify your credit card provider as soon as you discover that your card has been lost or stolen, or you may not be refunded for the full amount of any fraudulent spend.

Reporting fraudulent activity

If you believe your card or PIN has been taken or used fraudulently:

- Tell your credit card provider immediately
- Consider reporting the fraud to Action Fraud to get a police crime reference number
- Your credit card provider will cancel your card and send you a replacement
- If you believe someone else knows your PIN, you will be sent a new one

To help keep your money safe when abroad, take your card provider's helpline number with you when you travel. That way, you can call your provider immediately if a problem arises while you are away. These numbers are usually on the back of your card, but it's a good idea to have a note of them elsewhere.

What are you covered for?

Your responsibilities

As long as you exercise reasonable care and use your credit card safely, you should be protected if it is used fraudulently without your knowledge.

Your liability

Your credit card provider should refund the full amount if your card is used fraudulently. If your credit card provider believes you have not taken reasonable care, you may have to pay some of the fraudulent transaction.

If your provider refuses to refund you because it believes you've been negligent or were involved in the fraud, they will need to prove this.

Making a claim

If your credit card provider refuses to reimburse you, you may wish to put your request in writing. If you still do not get a refund, you can submit a claim to the Financial Ombudsman Service.

Identity theft protection

Identity theft can have serious consequences for your credit score and your ability to secure credit on good terms in the future.

- You have the option to request a free 90-day alert from the credit reference agencies.
- This can be useful if you think you're at risk of identity theft or fraud, or have already been a victim.
- The credit reference agencies will help you restore your credit score if it's affected by fraud.

Identity theft protection is also available, with policies typically providing access to free credit checks and an ID theft helpline.

Keeping your card provider informed

Unusual activity on your credit card may be refused and this can trigger a call from your provider's fraud team.

Make sure your provider always has an up-to-date mobile number for you, so they can reach you straightaway if there's a need to query a transaction.

To avoid genuine transactions being stopped, you can let your provider know in advance if you will be making unusually large purchases or using your credit card abroad.

Where else can you get help?

For more information on how to protect yourself against fraud, visit the Financial Fraud Action UK website.

1) http://www.sainsburysbank.co.uk/credit_cards/pin-numbers.shtml
2) http://www.financialfraudaction.org.uk/consumer-fraud-prevention-advice-remote-banking.asp?pagecontent=5
3) https://www.visa.co.uk/products/protection-benefits/verified-by-visa/how-to-use-verified-by-visa
4) http://www.mastercard.co.uk/securecode.html
5) https://www.americanexpress.com/uk/content/benefits/safekey.html
6) http://www.legislation.gov.uk/ukpga/1974/39/section/75
7) http://www.actionfraud.police.uk/
8) http://www.sainsburysbank.co.uk/library/default/resources/keeping-your-money-safe-abroad.pdf
9) http://www.financialfraudaction.org.uk/

This PDF aims to be informative and engaging. Though it includes tips and information, it does not constitute advice and should not be used for any financial decisions. Sainsbury's Bank accepts no responsibility for the content of external websites included within this PDF.

Terms & conditions

Sainsbury's Bank plc, Registered Office, 33 Holborn, London EC1N 2HT (registered in England and Wales, no. 3279730) is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Register no. 184514). Sainsbury's Supermarkets Ltd is an appointed representative of Sainsbury's Bank plc. Sainsbury's Bank plc is covered by the Financial Services Compensation Scheme (FSCS).

All information was correct at date of publication. This guide was updated and published on 3 September 2015.