



Bank card and cheque fraud

Bank card and cheque fraud happens when criminals steal your cards or chequebook and gain access to funds in your account.

More about bank card and cheque fraud

Criminals steal your bank cards or cheque book; or they obtain your card or account details, allowing them to take money from your account or run up credit in your name. You'll usually notice this by seeing unfamiliar transactions on your statements, or suddenly finding that you've exceeded your overdraft limit or credit limit and your card is refused when you try to make a purchase. Here are some of the ways a fraudster could steal money from you:

ATM (cash machine) fraud

A fraudster uses a device to capture your card information as you are withdrawing money from an ATM. The fraudster then uses this information to take money from your account in a shop, online or from an ATM.

Counterfeit cards

A fraudster counterfeits your bank card by using a device to capture the card and account information embedded in your card's magnetic strip. This is often known as 'skimming'. The fraudster then uses this information to carry out fraudulent transactions in countries where chip and PIN technology is not supported. The fraudster may also use this information in transactions where the card doesn't have to be physically seen by the retailer or merchant. For example, when shopping online; buying goods by telephone or mail order; or using cardholder activated terminals, such as ticket machines.

Lost or stolen card fraud

In this case, fraudsters use your card before you are able to report it as lost or stolen. A new or replacement card may also be stolen before you receive it. For example, if you have moved address recently and not had your mail redirected; or if your mail is delivered to a communal mailbox.

0300 123 2040
actionfraud.org.uk





Bank card and cheque fraud

Identity fraud

A fraudster may have stolen enough information about your identity and financial affairs to take over your account or to impersonate you. The fraudster will gain access to your account after getting through security online, at a bank branch or call centre, or by teaming up with someone inside the organisation that holds your account. If the fraudster can impersonate you, he or she will open accounts in your name and then defraud them.

Cheque fraud

Cheque fraud operates in a number of ways. For example, a fraudster pays you for goods or services using a stolen cheque; or deposits a fraudulent or stolen cheque into your account; or steals individual cheques or a cheque book from you.

Are you a victim of bank card or cheque fraud?

Your cards or chequebook have been stolen or faked and you notice unfamiliar transactions on your statement, or you find out that your overdraft limit is suddenly exceeded.

What should you do if you're a victim of bank card or cheque fraud?

- 👉 Immediately report lost or stolen cards or suspected fraudulent use of your card to your card company. You should also report lost or stolen cheque books or any missing cheques. Banks and companies have 24-hour emergency numbers printed on account statements.
- 👉 Report the offence to the relevant bank or card company, which will then be responsible for reporting the matter to the police. If the theft of your cards or cheques involved another crime – for example, if your bag was also stolen – you should make sure it is reported to the police.
- 👉 If a fraudulent account has been set up in your name and you don't have a relationship with that bank or card company, you can report the fraud directly to Action Fraud.

0300 123 2040
actionfraud.org.uk





Bank card and cheque fraud

- 👉 Remember to keep a record of all communications.
- 👉 Get a copy of your personal credit report from one of the credit reference agencies:
 - Callcredit (www.callcredit.co.uk)
 - Equifax (www.equifax.co.uk)
 - Experian (www.experian.co.uk)
- 👉 Consider contacting CIFAS – the UK’s Fraud Prevention Service (www.cifas.org.uk) to apply for protective registration. Once you have registered, CIFAS members will carry out extra checks whenever anyone applies for a financial service using your name and address.

Protect yourself against bank card and cheque fraud

Keep all your cards and financial details safe:

- 👉 look after your cards and card details at all times. Try not to let your card out of your sight when making a transaction
- 👉 check receipts against statements carefully. Contact your card company immediately if you find an unfamiliar transaction
- 👉 store your statements, receipts and financial documents safely and destroy them, preferably using a shredder, when you dispose of them
- 👉 sign any new cards as soon as they arrive
- 👉 cut expired cards through the magnetic strip and chip when replacement cards arrive.

Secure your PIN:

- 👉 memorise your PIN and destroy any paper notification as soon as you receive it

0300 123 2040
actionfraud.org.uk





Bank card and cheque fraud

- 👉 ensure that you're the only person that knows your PIN. Never write it down or record it. Your bank or the police will **never** phone you and ask you to disclose your PIN
- 👉 when entering your PIN, use your free hand and your body to shield the number from prying eyes or hidden cameras. If you think someone has seen your PIN or if you want to change it to something more memorable, you can change it at a cash machine (ATM) or by contacting your bank.

Take care when using cash machines:

- 👉 put your personal safety first. If someone makes you feel uncomfortable, cancel the transaction and use a different machine
- 👉 if you spot anything unusual about the cash machine, or if there are signs of tampering, don't use it. Report it to the bank concerned immediately
- 👉 be alert. If someone is crowding or watching you, cancel the transaction and go to another machine. Don't accept help from seemingly well-meaning strangers and never allow yourself to be distracted
- 👉 once you've completed a transaction, put your money and card away before leaving the cash machine. If the cash machine doesn't return your card, report its loss immediately to your card company. Destroy or preferably shred your cash machine receipt, mini-statement or balance enquiry when you dispose of them.

Take extra care when using cards abroad.

Before you go away:

- 👉 only take cards with you that you intend to use; leave others in a secure place at home
- 👉 make sure you have made a note of your card company's 24-hour contact phone number
- 👉 make sure your card company has up-to-date contact details for you, including a mobile number if possible

0300 123 2040
actionfraud.org.uk





Bank card and cheque fraud

- 👉 if your cards are registered with a card protection agency, ensure you have their contact number and your policy number with you.

When you are away:

- 👉 take the same precautions as you would in the UK. Look after your cards and card details, and shield your PIN with your free hand when typing it into a keypad in a shop or at a cash machine
- 👉 consider wearing a concealed money belt to keep your cards, cash and traveller's cheques safe.

When you get back:

- 👉 check your card statements carefully for unfamiliar transactions
- 👉 if there are any, report them to your card company as soon as possible.

When banking online:

- 👉 make sure your computer has up-to-date anti-virus software and a firewall installed. Think about using anti-spyware software. Download the latest security updates, known as patches, for your browser and for your operating system
- 👉 before you bank online, ensure that the locked padlock or unbroken key symbol is showing in your browser. When a connection is secure, the beginning of your bank's internet address should change from 'http' to https'
- 👉 be wary of unsolicited emails - known as phishing emails - asking for personal financial information. Your bank or the police would never contact you to ask you to disclose your PIN
- 👉 ensure your browser is set to the highest level of security notification and monitoring. The safety options are not always activated by default when you install your computer
- 👉 always access internet banking sites by typing the bank's address into your web browser. Never go to a website from a link in an email and then enter your personal details.

0300 123 2040
actionfraud.org.uk

action
fraud 
report and support



Bank card and cheque fraud

When shopping online:

- 👉 sign up to Verified by Visa or MasterCard SecureCode whenever you're given the option while shopping online. This involves you registering a password with your card company
- 👉 only shop on secure sites. Before submitting your card details, ensure the locked padlock or unbroken key symbol is showing in your browser. The retailer's internet address will change from 'http' to 'https' when a connection is secure
- 👉 never send your PIN over the internet
- 👉 print out your order and keep copies of the retailer's terms and conditions, returns policy, delivery conditions, postal address (not a post office box) and phone number (not a mobile number).



0300 123 2040
actionfraud.org.uk

**action
fraud** 
report and support