Banking and credit card fraud

FACT SHEET

What is banking and credit card fraud?

Banking and credit card fraud happens when personal information is stolen from your debit, credit or store card, or the card itself is stolen, in order for money to be taken from your account or used to buy items in your name.

What can be done if you are a victim?

- If you paid via bank transfer or debit card, contact your bank to discuss the possibility of getting your money back. There is no guarantee that your bank can do this.
- If you bought something that costs between £100 to £30,000 on your credit card, you may be entitled to your money back under the Consumer Credit Act 1974.
- Action Fraud cannot speak to the bank on your behalf or close down accounts.
- In some cases the police and other law enforcement agencies may want to contact you for further details so it is important that you keep any relevant information about the crime.
- It is difficult for police to investigate every instance of fraud – prevention and protection is a far better method of dealing with it. By taking some simple steps, you can avoid falling victim in the future.

How to protect yourself

- Look after your cards – keep them with you everywhere you go. Never hand over a card, particularly if you're paying using a contactless card machine.
- Be protective of your banking information. Either store your statements, receipts and documents safely or destroy them using a shredder.
- Sign new cards as soon as they arrive and cut up old cards through the magnetic strip and the chip once they've expired or been cancelled.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Banking and credit card fraud

FACT SHEET

When banking online:

- Make sure your computer has up-to-date anti-virus software and a firewall installed. Consider 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 will never ask you to disclose your PIN.
- 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.

What should you do if you've been a victim of bank card fraud?

- Immediately report lost or stolen cards or suspected fraudulent use of your card to your card company. Banks and companies have 24-hour emergency numbers printed on account statements.
- 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.com**)
  Experian (**www.experian.co.uk**)
  ClearScore: (**www.clearscore.com**)
  Noddle: (**www.noddle.co.uk**)

- Consider contacting Cifas – the UK's Fraud Prevention Service 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. (**www.cifas.org.uk**)

Report and get advice at:

www.actionfraud.police.uk

Other places for help and advice:

www.getsafeonline.org
www.cyberaware.gov.uk

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk