

# Personal Security Plan

The best ways to minimise your chances  
of becoming a victim of fraud



# Contents

Introduction	03
Types of fraud	
Plastic card fraud	04
Cash machine fraud	08
Cheque fraud	10
Online fraud	12
Identity fraud	16
Industry fraud prevention measures	18
Useful contacts	19

# Introduction

With the flexibility of payments becoming ever greater, everyone needs to be aware of the common sense steps that should be taken to minimise the chances of being a fraud victim – whether it is in a shop, online or over the phone. However, fraud can cause stress and worry, so taking measures to protect yourself is essential. Luckily, it only takes a few easy steps to make it much harder to be defrauded. This guide provides details on the ways in which fraudsters operate, and useful advice on how to better protect yourself.



# Plastic card fraud

Cards are safer to use than cash. APACS figures show that fraudulent card transactions make up just 0.095% of all plastic card transactions. If you are unlucky enough to become a victim of fraud the good news is that you are protected by *The Banking Code* and should not suffer any financial loss as a consequence – provided you have not acted fraudulently or without reasonable care (e.g. you haven't written down your PIN and haven't disclosed it to someone else).

Criminals are always looking for ways to get hold of your cards, PINs and card details and the industry is committed to fighting fraud on all fronts. Chip and PIN has made our cards

much less likely to be used fraudulently in UK shops and businesses. Efforts continue to tackle fraud in other situations such as internet and phone shopping.

## Help

Online advice initiatives such as Card Watch aim to raise awareness of card fraud prevention. For comprehensive information on fraud prevention – including types of fraud, how common they are and what is being done to combat it – visit the Card Watch website at [www.cardwatch.org.uk](http://www.cardwatch.org.uk)

### Plastic card fraud losses on UK-issued cards split by fraud type

Fraud Type	2006 (+/-change on 2005)	2005	2004
Counterfeit (skimmed/cloned) card fraud	£99.6m (+3%)	£96.8m	£129.7m
Fraud on stolen or lost cards	£68.4m (-23%)	£89.0m	£114.5m
Card-not-present fraud (phone/internet/mail)	£212.6m (+16%)	£183.2m	£150.8m
Mail non-receipt	£15.4m (-62%)	£40.0m	£72.9m
Card ID theft	£31.9m (+5%)	£30.5m	£36.9m
<b>TOTAL</b>	<b>£428.0m (-3%)</b>	<b>£439.4m</b>	<b>£504.8m</b>
<b>Contained within this total:</b>			
UK retailer (face-to-face transactions)	£72.1m (-47%)	£135.9m	£218.8m
Cash machine fraud	£61.9m (-6%)	£65.8m	£74.6m
<b>Domestic/International split of total figure:</b>			
UK fraud	£309.8m (-13%)	£356.6m	£412.3m
Fraud abroad	£118.2m (+43%)	£82.8m	£92.5m

NB: Figures have been rounded to one decimal place

## Types of plastic card fraud

The main types of credit and debit card fraud are:

- **Card-not-present (CNP) fraud:** This occurs when fraudsters use stolen card details to buy goods or services online, by phone or mail order. Due to the success of chip and PIN in reducing fraud on the high street, this is now the most common type of card fraud in the UK. The challenge in countering this type of fraud lies in the fact that neither the cardholder nor the card is present when the transaction happens.
- **Counterfeit card fraud:** This occurs when fraudsters make an illegal copy of your credit or debit card's magnetic stripe. It is not a new scam and does not undermine chip security. Most of this fraud involves skimming, whereby your card's magnetic stripe data (on the back of the card) is electronically copied by a criminal. Fraudsters skim cards by using a hand-held device, or one that is fitted to a cash machine or a PIN pad. This data is then transferred onto a fake card.

A counterfeit card can potentially be used in stores that haven't upgraded to chip and PIN or at an overseas cash machine that hasn't been upgraded to chip and PIN – although to use a fake card at a foreign cash machine a

criminal will also need to have obtained your PIN by separate means. Often you will be unaware of this fraud until a statement arrives, showing purchases or cash withdrawals that you did not make.

- **Lost and stolen card fraud:** This occurs when your debit or credit card is physically stolen or lost and then used by a criminal, posing as you. Most of this fraud takes place before you realise your card has been stolen or before you have reported it lost. Lost and stolen card fraud has been steadily decreasing since the introduction of chip and PIN.
- **Card ID theft:** This occurs when a criminal has managed to obtain details other than just your credit or debit card, such as stolen personal information, to open or take over a card account in your name.
- **Mail non-receipt card fraud:** This type of fraud occurs when your new card – being sent to you by your card company – is stolen by fraudsters. Those most at risk from this type of fraud are people with communal letterboxes, such as those living in flats and student accommodation or people who have moved and not redirected their post.

## Securing your plastic cards: top tips

To minimise the chances of becoming a victim of card fraud:

- Look after your cards and card details at all times.
- Try not to let your card out of your sight when making a transaction.
- Never leave your cards unattended, e.g. in a bag, briefcase or jacket pocket in a public place.
- Check receipts against statements carefully. If you find an unfamiliar transaction, contact your card company immediately.
- Store your statements, receipts and documents that contain information relating to your financial affairs safely and destroy or preferably shred them when you dispose of them.
- Sign any new cards as soon as they arrive.
- Cut expired cards through the chip first and then the magnetic stripe when replacement cards arrive.
- Pay attention to card expiry dates. If your replacement card hasn't arrived call your bank or building society to check the status of your new card.
- Report lost or stolen cards or suspected fraudulent use of your card to your card company immediately. The 24-hour emergency number is on your last statement or call directory enquiries.
- As of 1 April 2007, if you are the victim of plastic card, cheque or online banking fraud you should only report the offence to the relevant bank or card company. The responsibility then lies with your bank or card company – and not you – to report the matter to the relevant regional police force. Therefore it will be up to the financial institution concerned to get a crime reference number if they consider it appropriate.

## PIN security: safety in numbers

To ensure you protect your PIN:

- Ensure that you are the only person that knows your PIN. Your bank or the police will never phone you and ask you to disclose it. Never write it down or record it.
- When entering your PIN use your spare hand and your body to shield the number from prying eyes or hidden cameras. If you think someone has seen your PIN you can change it at a cash machine or by contacting your bank.
- Memorise your PIN and destroy any paper notification as soon as you receive it. If the PIN you are given is difficult to remember, change it to something more memorable.

### What happens if you become a victim of card fraud?

- If you suspect or discover that your card has been lost or stolen or that you have been the victim of a fraud tell your card company immediately.

- If someone else uses your card before you tell your card company it has been lost or stolen or before you tell them that someone else knows your PIN, the most you will have to pay, in theory, is £50. In practice your card company will usually refund the full amount lost. But if you are found to have acted fraudulently or without reasonable care, for example, by keeping your PIN written down with your card, you would have to meet all the losses yourself.
- If your card is used fraudulently before you receive it, you will not have to pay for any losses.



# Cash machine fraud

Cash machines are generally very safe but they sometimes attract criminal attention. Cash machine fraud has decreased by six per cent in the past year, but you still need to follow common sense precautions when withdrawing cash.

A number of initiatives are in place to tackle this type of crime. One is the introduction of privacy spaces, which comprise a zoned area marked on the ground in front of the cash machine to enable users to withdraw cash in private. This zone discourages people from standing too close to you when you are taking money out, and makes it easier to challenge anyone standing too close to you.



## Fact

There were more than 60,000 cash machines in the UK at the end of 2006. Britons make the largest number of cash machine withdrawals of any country in the EU – 2.75 billion transactions in total in 2006 – worth over £179 billion. The busiest day of the week at cash machines is Friday while the average amount we withdraw from a bank-owned machine is £65.

## Cash machine safety: top tips

To minimise your chances of someone getting your card or card details at a cash machine:

- Put your personal safety first. Be aware of others around you and if someone makes you feel uncomfortable cancel the transaction and use a different machine. If you spot anything unusual about the cash machine, or there are signs of tampering, do not 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. Do not accept help from seemingly well-meaning strangers and never allow yourself to be distracted.
- Stand close to the cash machine. Always shield the keypad with your spare hand and your body to avoid anyone seeing you enter your PIN.
- Once you have completed a transaction put your money and card away before leaving the cash machine. If the cash machine does not 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.
- Be aware that contrary to recent speculation, if you enter your PIN backwards at a cash machine it will NOT alert law enforcement of a potential threat. In such situations you should always put your personal safety first and comply with a criminal's demands.

# Cheque fraud

In 2006 cheque fraud losses totalled £30.6 million, a decrease of 24 per cent on the 2005 figure. Typical cheque fraud involves a criminal using counterfeit, forged or fraudulently altered cheques to pay for goods or services.

Most fraudulent or stolen cheques are successfully identified by the banking industry as they pass through the cheque clearing system. Currently, the industry identifies and stops more than 90 per cent of all fraudulent cheques, thereby preventing customers losing cash.

In November 2007, the banking industry is changing the way cheques are processed to benefit customers accepting cheques. It means that

for the first time you can be sure that after a maximum of six working days (after paying in a cheque) the money is yours and you are protected from any loss should the cheque turn out to be fraudulent. This means that the funds from a cheque cannot then be reclaimed without your permission, unless you are a knowing party to fraud.

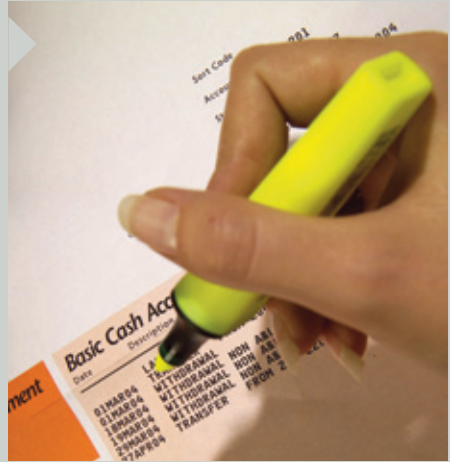
Despite this positive change the industry continues to recommend that you should be wary of accepting cheques or bankers' drafts if you don't know or trust the person offering them to you – particularly if they are of high value.

Any innocent customer whose chequebook is used by a fraudster will continue to enjoy full protection from any financial loss, provided they haven't breached their terms and conditions.



## Avoiding cheque fraud: top tips

- Never accept a cheque or bankers' draft from someone unless you absolutely know and trust them. Be especially wary when accepting a high-value cheque, for instance if you are selling a car. Consider other payment options such as a CHAPS, automated payment via BACS or cash. Also a new faster phone and internet payments service will be available from late 2007.
- Be aware that a bankers' draft is not necessarily safe from fraud. If you receive a bankers' draft in payment for goods you must allow time for the draft to clear before releasing the goods. Bankers' drafts can be stolen or altered like any other cheque and if it is altered, stolen or counterfeit it will not be honoured.
- Keep your chequebook in a safe place, report any missing cheques to your bank immediately and always check your bank statement thoroughly.
- If you are writing a cheque and making it payable to a bank or a building society, do not make the cheque payable simply to that organisation. Add further details in the payee line, for example XYZ Bank, re J Jones, account number 123456. (The rules for



- accepting cheques at banks and building societies changed in September 2006, in order to safeguard against fraud. If you try to deposit a cheque in a branch, or by post, made simply to a bank or building society, it may not be cleared and is likely to be returned.)
- Banks will examine each case of cheque fraud on an individual basis but, generally speaking, if you are an innocent victim of cheque fraud who has had a cheque or chequebook stolen and used fraudulently you will be refunded. However, if you have accepted a cheque or bankers' draft that turns out to be fraudulent you may be liable.

# Online fraud

Nearly 17 million people in the UK now regularly use the internet to access their bank accounts, and millions more regularly shop online.

Most fraud on online bank accounts involves a customer being duped into giving away their user passwords and security information. Typically this happens through a phishing scam or because the customer is using an inadequately protected PC that has enabled a fraudster to access their account. In 2006 online banking fraud amounted to £33.5 million of losses compared with £23.2 million in 2005.

## Shopping online

The incidence of computer hackers stealing and using cardholder data from retailer websites remains low. Similarly, the vast majority of online businesses are honest and legitimate and comply with their obligations to carefully protect and securely dispose of cardholder information. The reality is that most internet card fraud involves a criminal obtaining genuine card details in the real world that are then used to shop online.

## Fact

In 2006, three quarters (26.4 million) of all internet users in the UK made an online purchase. This is up from 50 per cent of internet users in 2002. In addition to the increase in the number of adults spending online, the number of purchases being made is growing – the average number of purchases made by online shoppers rose from 13.6 in 2004 to 18.5 in 2005 and to 23.2 in 2006.

## Fact

APACS research shows that:

- One in eight online shoppers have failed to log out when shopping online, leaving their financial details available to others
- One in four online shoppers do not check whether a website is safe and secure



## Shopping online: top tips

To minimise your chances of becoming a victim of fraud whilst shopping online, you should:

- Be aware that your card details are as valuable as cash in the wrong hands so store your cards securely at all times and try not to let them out of your sight.
- Sign up to Verified by Visa or MasterCard SecureCode whenever you are given the option whilst shopping online. This involves you registering a password with your card company. By signing up you will prevent fraudsters from using your card details on participating sites as they will not know your password.
- Only shop on secure sites. Before submitting card details ensure that the locked padlock or unbroken key symbol is showing in your browser. (The locked padlock symbol is usually found at the top of the screen if you use Internet Explorer 7 or Firefox 2.) The beginning of the online retailer's internet address will change from 'http' to 'https' when a connection is secure. In some new browsers, such as Internet Explorer 7 and Firefox 2, the address bar may also turn green to indicate that a site has an additional level of security.
- Never disclose your PIN to anyone and never send it 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). There may be additional charges such as local taxes and postage, particularly if you are purchasing from abroad. When buying from overseas remember that it may be difficult to seek redress if problems arise, but having all the aforementioned information will help your card company take up your case if you subsequently have any difficulties.
- Ensure you are fully aware of any payment commitments you are entering into, including whether you are instructing a single payment or a series of payments.
- Consider using a separate credit card specifically for online transactions.



## Banking online

In the UK over a third of the adult population (nearly 17 million people) – now bank online. Unsurprisingly more people are also using their online account more regularly – with one in five users going online daily compared to one in thirteen just four years ago.

Your chances of becoming a victim of online banking fraud are very low and banks are committed to keeping it this way. Because the banks' own systems have proven difficult to attack, criminals have turned their attention to getting information directly from online banking customers themselves. The two most common attempted scams currently used by online fraudsters are phishing and Trojans.

## Phishing

This is an e-mail that purports to be from your bank or another service such as PayPal, urging you to click on a link that takes you to a fake website identical to the one you would expect to see. You are then asked to verify your personal security information. If you submit this information you are actually giving it to a fraudster.

### Phishing: top tips

To avoid phishing scams you should:

- Always be suspicious of emails which are supposedly from your bank.
- Never give your login details in full by email or over the phone – your bank will never request these in this way.
- Report all phishing emails to [reports@banksafeonline.org.uk](mailto:reports@banksafeonline.org.uk).
- Make sure your home computer has a security programme and virus protection.

## Trojan

This is a type of computer virus which can be installed on your computer without your knowledge. It is capable of logging your keystrokes thereby capturing your passwords and other personal information. To make sure you don't become a victim of a trojan, always ensure you have up-to-date anti-virus software installed, and ask for technical support if your computer starts acting oddly.

## Further information

Other places that you can look to get useful information and advice about banking and shopping safely online include:

[www.banksafeonline.org.uk](http://www.banksafeonline.org.uk)  
[www.identitytheft.org.uk](http://www.identitytheft.org.uk)  
[www.getsafeonline.org.uk](http://www.getsafeonline.org.uk)  
[www.consumerdirect.gov.uk](http://www.consumerdirect.gov.uk)  
[www.visaurope.com/verified](http://www.visaurope.com/verified)  
[www.mastercard.co.uk/securecode](http://www.mastercard.co.uk/securecode)

## Banking online: top tips

To help avoid online scams you should always:

- Make sure your computer has up-to-date anti-virus software and a firewall installed. Consider using anti-spyware software. You should also download from the internet the latest security updates, known as patches, for your browser and for your operating system (e.g. Windows).
- Be wary of unsolicited emails requesting personal financial information. Keep passwords and PINs safe; always be wary of unsolicited emails or calls asking you to disclose any personal details or card numbers. Your bank, building society or the police would never contact you to ask you to disclose your PIN or any of your password information.

As additional preventative measures when banking online you are also encouraged to:

- Make sure 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.
- Know who you are dealing with – 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 personal details.
- Report phishing emails to [reports@banksafeonline.org.uk](mailto:reports@banksafeonline.org.uk)

# Identity fraud

This fraud involves criminals obtaining key pieces of personal information that they use to pretend to be you. Criminals use these personal details to obtain financial services products in your name such as credit cards, loans and mortgages. Alternatively criminals can use your personal information to gain access to your existing accounts.

APACS has worked closely with the Home Office to develop [www.identitytheft.org.uk](http://www.identitytheft.org.uk), which provides practical advice on how to avoid becoming an ID theft victim and what to do if you do become a victim.

## Avoiding identity fraud: top tips

To help ensure you keep your identity safe, you should:

- Always keep important personal documents, plastic cards and chequebooks in a safe and secure place. Without access to this information a criminal will find it very difficult to pretend to be you.
- Don't share personal information unless you are entirely confident you know who you are dealing with.
- Store your statements, receipts and documents that contain information relating to your financial affairs safely and destroy or preferably shred them when you dispose of them.
- Always check bank statements, and check receipts against your statements carefully. If you find an unfamiliar transaction contact your card company or bank immediately.
- Be aware that your post is valuable information in the wrong hands. If you fail to receive a bank statement, card statement, utility bill or other financial information contact the supplier.
- Get your post redirected to your new address if you move house.
- Guard your cards. Don't let them out of your sight when making a transaction. Report lost and stolen cards, or suspected fraudulent use of your card account to your bank or building society immediately.

## If you have become a victim: top tips

Steps to take if you find you have become a victim of fraud:

- If the fraud involves credit or debit cards, online banking or cheques, you should report it to the financial institution concerned. They will then be responsible for undertaking further investigation and, as appropriate, reporting cases of criminal activity directly to the police. Therefore it will be up to the financial institution concerned to get a crime reference number if they consider it appropriate.
- If the fraud has not involved credit or debit cards, online banking or cheques then you should report the matter to the relevant organisation in the first instance, and, dependent on their advice, then to your local police station.
- Ensure you keep a record of all communications.
- Contact the credit reference agencies Experian, Equifax and Call Credit (see page 19). If applications for credit have been made in your name you can ask to have any incorrect information removed.
- It is useful to obtain a regular copy of your credit report – perhaps annually. A paper copy of your report is available from any of the above agencies for £2.
- Contact CIFAS on 0870 010 2091. They will earmark your name and address so that anyone applying for something using your name will automatically be double-checked.
- If you suspect mail theft contact the Royal Mail Customer Enquiry Number on 08457 740740.



## Industry fraud prevention measures

A number of fraud prevention measures are in place to tackle all types of fraud and the banking industry continues to work with the retail industry, law enforcement and the Home Office on other ways to tackle fraud across a range of payment methods. Initiatives in place include:

- The £1.1 billion investment in chip and PIN.
- Establishment of the special police squad, the Dedicated Cheque and Plastic Crime Unit (DCPCU), that specifically tackles plastic card and cheque fraud – a funding commitment of £3m per year by the banking industry.
- An automated cardholder address verification and card security code system to help businesses that accept internet and phone transactions.
- Online secure payment systems such as MasterCard SecureCode and Verified by Visa.
- The Industry Hot Card File – an industry database that enables retailers to electronically check whether a card is being used fraudulently. Over 430,000 cases of attempted fraud were prevented by this system in 2005.
- Banks' use of intelligent fraud-detection systems that spot fraud by checking for unusual spending patterns on cards.
- Publication of a range of fraud prevention and educational materials available free-of-charge for businesses throughout the UK.
- Constant evaluation and trialling of the next generation of fraud prevention solutions. One example is the use of a chip and PIN card with a hand-held reader to generate a one-time only passcode in order to make online banking, and shopping over the internet and telephone even safer.

## Useful contacts

**www.bankingcode.org.uk** – a body that ensures that banks and building societies comply with the standards detailed in *The Banking Code* and *The Business Banking Code*.

**www.banksafeonline.org.uk** – assistance for internet users to help them protect themselves from online scams and threats such as phishing.

**www.callcredit.co.uk** – a credit reference agency with a range of information services for businesses and individuals. (Tel: 0870 060 1414).

**www.cardwatch.org.uk** – information about how card fraud takes place in the UK, what is being done to prevent it and how you can help prevent yourself from becoming a victim.

**www.chipandpin.co.uk** – information, guidance and downloadable materials for businesses and customers about chip and PIN.

**www.cifas.org.uk** – the UK's fraud prevention service, which enables its members to share information on fraudulent activity to help identify and prevent fraud taking place, including on card accounts.

**www.consumerdirect.gov.uk** – clear and practical help and advice for consumers in Great Britain.

**www.equifax.co.uk** – a credit reference agency that provides information to businesses, consumers and the public sector. (Tel: 0870 010 0583).

**www.experian.co.uk** – a credit reference agency that helps consumers, businesses and the public sector manage their credit information. (Tel: 0870 241 6212).

**www.financial-ombudsman.org.uk** – an independent service for resolving disputes between consumers and financial firms.

**www.getsafeonline.org** – a Government and leading business-sponsored site that provides advice on how to protect your computer and use the internet with safety.

**www.identitytheft.org.uk** – how to help protect yourself from identity theft, what to do if it happens to you and suggestions on where to get further help.

**www.mastercard.com/uk/securecode** – details of how to sign up and benefit from extra protection when shopping online with a MasterCard.

**www.oft.gov.uk** – provides information and advice for consumers about your rights when shopping, scams to avoid and where to go for help and assistance.

**www.visaeurope.com/verified** – details of how to sign up and benefit from extra protection when shopping online with a Visa card.

For further information please contact:

APACS  
Mercury House  
Triton Court  
14 Finsbury Square  
London  
EC2A 1LQ  
Tel 020 7711 6259  
Fax 020 7256 5527

Email: [press@apacs.org.uk](mailto:press@apacs.org.uk)  
[www.apacs.org.uk](http://www.apacs.org.uk)

APACS (Administration) Limited 2007

