

# Cash Machine Fraud Prevention Guide

July 2010

More than 70% of the cash in our pockets comes from a cash machine. To meet this demand there are more than 63,000 cash machines across the UK with 8 million cash withdrawals made from them every day. Although using a cash machine is generally very safe, cash machines – just like our wallets, handbags, cars and houses – are sometimes targeted by criminals. This guide explains the main types of fraud that take place at cash machines and provides some simple advice on how you can protect yourself and your cards.

## How cards and card details are stolen at cash machines

There are three main ways in which criminals try to steal cards, card details and PINs at cash machines.

- **Card-trapping devices** – a device is temporarily inserted into a cash machine's card entry slot by a criminal. The device traps a customer's card in the machine, not allowing the transaction to be processed. The criminal will also attempt to find out the PIN, so cardholders who do not shield the keypad are at much greater risk of this type of fraud than those who do.

Criminals attempt to get hold of the PIN either by: looking over the customer's shoulder; via a miniature pinhole camera fixed above the keypad; or the criminal may even pretend to be a well-meaning bystander who convinces the customer to re-enter the PIN while they watch. The customer then

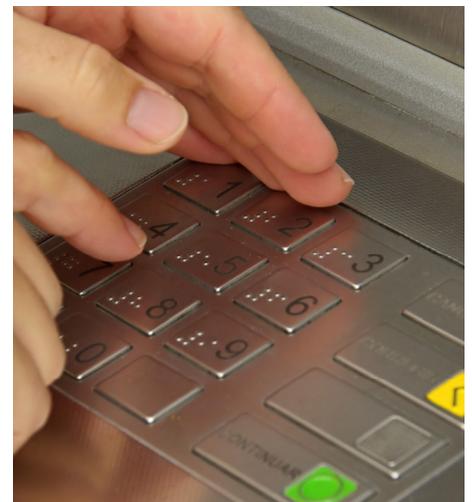
gives up on the transaction, thinking that their card has been retained, and walks away from the machine. The criminal then removes the device, along with the customer's card, which they use with the PIN to withdraw cash or to buy high-value goods in shops.

- **Skimming and pinhole camera devices** – skimming is the term used to describe how a criminal copies a card's electronic data. A criminal fits a skimming device over the cash machine's card entry slot to copy the magnetic stripe details of a customer's card as the customer inserts it into the machine. The criminal will also try to get hold of the cardholder's PIN and sometimes will have attached a miniature camera above the keypad to film the customer entering their PIN. Many customers will not notice these devices and will make their withdrawals as normal. The criminal uses the copied details to make a fake magnetic stripe card, which will be used - with the genuine PIN - at foreign cash machines or shops that haven't yet been upgraded to chip

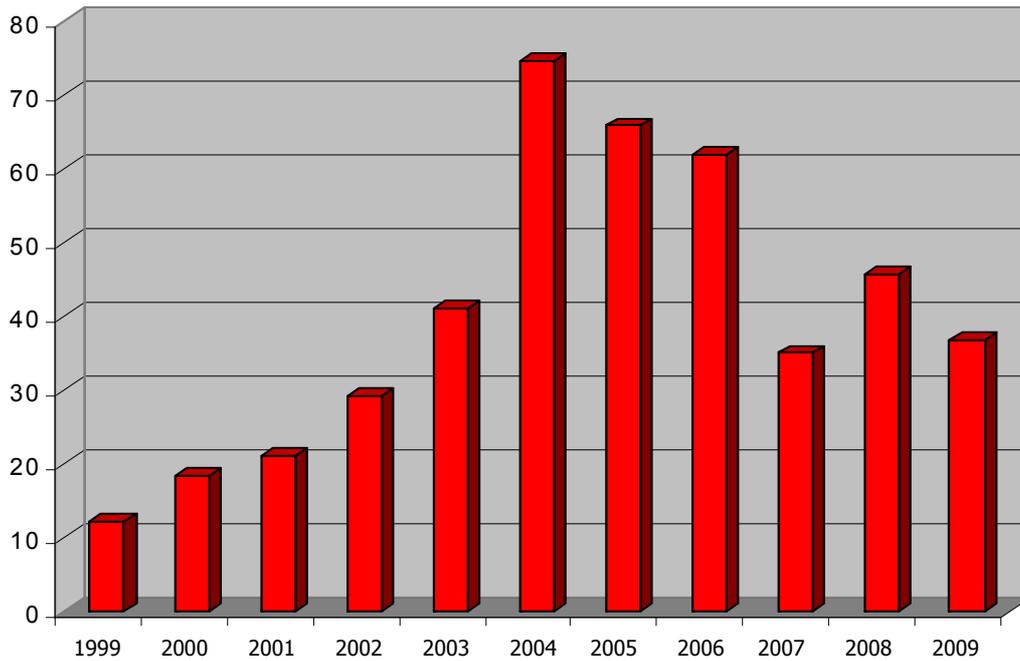
and PIN. Customers who shield the keypad when they enter their PIN are much less likely to fall victim to this type of fraud.

- **Shoulder-surfing** – a criminal watches the cardholder enter their PIN, then subsequently steals their card using distraction techniques or pick pocketing, before using the stolen card and genuine PIN.

Cardholders who do not cover the keypad when they enter their PIN may be vulnerable to this type of crime.



## Fraud losses at UK cash machines 1999-2009 (£ millions)



The amount of money withdrawn fraudulently from our cards at UK cash machines fell 20 per cent in 2009, to £36.7 million - a small fraction compared with the £193 billion withdrawn through cash machines in 2009.

# Stay safe from fraud when using a cash machine

Cash machines are generally very safe but there are some very simple steps you can take to make them safer still.

### Protect your PIN

The simplest step of all to minimise the chances of falling victim to fraud is to shield the keypad when you enter your PIN. This will protect your PIN from a shoulder-surfer, and also if a criminal has set up a hidden camera that is filming the keypad.

Some losses at UK cash machines are still, unfortunately, the result of PINs being written down and kept in a purse or wallet. So, the other important advice remains: 'never write down your PIN'.

### Choosing a Cash Machine

- Be aware of others around you. If someone close to the cash machine is behaving suspiciously, or makes you feel uncomfortable, go to another machine.

- If you suspect that a skimming device has been attached to a cash machine, inform staff within the bank or, if this is not possible, inform the police.



### Using a cash machine

- Be aware of your surroundings. If someone starts crowding or watching you, cancel the transaction, preferably before you've entered your PIN, and go to another machine.
- Stand close to the cash machine and always shield the keypad effectively, for example by using your free hand, to avoid anyone seeing you enter your PIN. If your card gets jammed or retained by the machine report this as soon as possible to your card issuer.

### Leaving a cash machine

- Discreetly put your money and card away before leaving the cash machine.

## What to do if you are a victim

If you are a card fraud victim you should report it to your card issuer as soon as possible. They will then be responsible for undertaking further investigation and, as appropriate, reporting the fraud directly to the police.

### Will you get your money back?

If you are a victim of card fraud you are protected through legislation, which states that you will not be liable for losses unless you have acted fraudulently or without reasonable care.

### What is being done to prevent cash machine fraud?

LINK, the UK's cash machine network, and the UK banking industry continue to work on a number of initiatives to deter, detect and prosecute the fraudsters.

- Working with cash machine suppliers on technical enhancements to prevent cash machine tampering. This includes redesigned card reader surrounds in order to make it difficult to attach a skimming device.
- Ensuring all UK cash machines are upgraded to chip and PIN. This programme is complete in the UK and has helped to reduce cash machine fraud losses by 51% in the past six years.
- Working with the police to target the organised criminals behind these types of crime, including a reward scheme with Crimestoppers (see below).
- The widespread introduction of PIN-change functionality at UK cash machines, so that cardholders who think their PIN may have been observed can change it easily and quickly.
- Providing consumer advice on best practice when using a cash machine. This includes co-ordinated use of screen messages designed to raise cash machine users' awareness of fraud prevention good practice, such as shielding your PIN, and reporting capture of a card as soon as possible.
- Extensive use of CCTV to deter and detect criminal activity.

### Cash reward programme to combat cash machine crime

To help combat cash machine crime LINK works with Crimestoppers, the independent charity, to offer rewards for information relating to cash machine crime. Working closely with different police agencies and departments, including the Dedicated Cheque and Plastic Crime Unit - a banking industry-sponsored special police unit - the partnership aims to support the police in their fight against crime and help inform the public about how they can protect themselves.

LINK offers rewards of up to £25,000 for information relating to cash machine crime. Anyone with details about those responsible can call Crimestoppers on 0800 555 111, or visit their website [www.crimestoppers-uk.org](http://www.crimestoppers-uk.org) where you can leave your information completely anonymously.

## Facts and Figures

- There are more than 63,000 cash machines in the UK.
- The busiest day of the week at cash machines is Friday.
- In 2009 the average amount withdrawn per cash machine visit was £66.
- The total value of all withdrawals from ATMs reached £193 billion in 2009.
- In 2009, there were 34.7 million regular users of cash machines compared with 26.1 million in 1997.
- Last year 97% of cash machine withdrawals were from free-to-use cash machines.
- Cash machine fraud losses decreased by 20% in 2009.

## Useful Links

[www.link.co.uk](http://www.link.co.uk)

[www.financialfraudactionuk.org.uk](http://www.financialfraudactionuk.org.uk)