Financial Fraud Action UK is the name under which the financial services industry co-ordinates its activity on fraud prevention, presenting a united front against financial fraud and its effects. Financial Fraud Action UK works in partnership with The UK Cards Association on industry initiatives to prevent fraud on credit and debit cards, with the Fraud Control Steering Group on non-card fraud matters and the Cheque and Credit Clearing Company on credit clearing and cheque fraud.

The UK Cards Association is the leading trade association for the card payments industry in the UK. With a membership that includes all major credit, debit and charge card issuers, and card payment acquirers, the Association contributes to the development of legislative and regulatory frameworks; develops industry best practice; safeguards the integrity of card payments by tackling card fraud; develops industry standards; and co-ordinates other industry-wide initiatives across matters relating to both card payments and the provision of credit.

The Cheque and Credit Clearing Company is a membership-based industry body which manages the cheque clearing system in Great Britain. It also covers the management of the systems for clearing paper bank giro credits (the credit clearing), Euro-denominated cheques (the euro clearing) and US Dollar cheques (the currency clearing for US dollar cheques drawn on GB banks).

The Fraud Control Steering Group is an unincorporated association of financial institutions who participate in retail banking and the payments market in the UK. It is responsible for formulating and implementing policy and ensuring a coordinated industry approach to fighting payment, cheque and lending fraud.
“Driving down fraud and keeping cards safe continues to be a priority for the industry. This is the third year card fraud losses have fallen – clear proof that our endeavours to fight fraud are packing a punch. Customers have also played their part in driving down losses by taking heed of advice about looking after their personal and financial details.”

MELANIE JOHNSON, Chair of The UK Cards Association

“The large decrease in online banking fraud this year is extremely encouraging. It shows the efforts of everyone involved in combatting this type of fraud are paying off. But we remain committed to our on-going work with key partners to reduce all areas of fraud, and to ensure that our customers can continue to enjoy great protection when they use online and telephone banking.

DAVID COOPER, Chairman of the Fraud Control Steering Group
FRAUD LOSSES ON UK-ISSUED CARDS 2001-2011
Tinted figures show percentage change on previous year’s total
ANNUAL FRAUD LOSSES ON UK-ISSUED CARDS 2001-2011
All figures in £ millions

<table>
<thead>
<tr>
<th>Fraud type</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>+/- change 10/11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card-not-present</td>
<td>95.7</td>
<td>110.1</td>
<td>122.1</td>
<td>150.8</td>
<td>183.2</td>
<td>212.7</td>
<td>290.5</td>
<td>328.4</td>
<td>266.4</td>
<td>226.9</td>
<td>220.9</td>
<td>-3%</td>
</tr>
<tr>
<td>Counterfeit</td>
<td>160.4</td>
<td>148.5</td>
<td>110.6</td>
<td>129.7</td>
<td>96.8</td>
<td>98.6</td>
<td>144.3</td>
<td>169.8</td>
<td>80.9</td>
<td>47.6</td>
<td>36.1</td>
<td>-24%</td>
</tr>
<tr>
<td>Lost/stolen</td>
<td>114.0</td>
<td>108.3</td>
<td>112.4</td>
<td>114.4</td>
<td>89.0</td>
<td>68.5</td>
<td>56.2</td>
<td>54.1</td>
<td>47.7</td>
<td>44.4</td>
<td>50.1</td>
<td>+13%</td>
</tr>
<tr>
<td>Card ID theft</td>
<td>14.6</td>
<td>20.6</td>
<td>30.2</td>
<td>36.9</td>
<td>30.5</td>
<td>31.9</td>
<td>34.1</td>
<td>47.4</td>
<td>38.2</td>
<td>38.1</td>
<td>22.5</td>
<td>-41%</td>
</tr>
<tr>
<td>Mail non-receipt</td>
<td>26.8</td>
<td>37.1</td>
<td>45.1</td>
<td>72.9</td>
<td>40.0</td>
<td>15.4</td>
<td>10.2</td>
<td>10.2</td>
<td>6.9</td>
<td>8.4</td>
<td>11.3</td>
<td>+34%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>411.5</td>
<td>424.6</td>
<td>420.4</td>
<td>504.8</td>
<td>439.4</td>
<td>427.0</td>
<td>535.2</td>
<td>609.9</td>
<td>440.0</td>
<td>365.4</td>
<td>341.0</td>
<td>-7%</td>
</tr>
</tbody>
</table>

Contained within this total/breakdown by location

<table>
<thead>
<tr>
<th>Location</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>+/- change 10/11</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK</td>
<td>273.0</td>
<td>294.4</td>
<td>316.3</td>
<td>412.3</td>
<td>356.6</td>
<td>309.9</td>
<td>327.6</td>
<td>379.7</td>
<td>317.4</td>
<td>271.5</td>
<td>261.0</td>
<td>-4%</td>
</tr>
<tr>
<td>Fraud abroad</td>
<td>138.4</td>
<td>130.2</td>
<td>104.1</td>
<td>92.5</td>
<td>82.8</td>
<td>117.1</td>
<td>207.6</td>
<td>230.1</td>
<td>122.6</td>
<td>93.9</td>
<td>80.0</td>
<td>-15%</td>
</tr>
</tbody>
</table>

Due to the rounding of figures, the sum of separate items may differ from the totals shown.
08 // PLASTIC CARD FRAUD

OVERVIEW

Total fraud losses on UK cards fell by seven per cent between 2010 and 2011 to £341 million. This is the lowest annual total since 2000 and follows on from a fall of 17 per cent in the previous year. Whilst card usage and transaction volumes continue to grow, card fraud losses against total turnover – at 0.06% – continue to decrease and have now fallen by 33 per cent in the past two years.
FRAUD TO TURNOVER RATIO 2001-2011
Tinted figures show percentage change on previous year’s total
PLASTIC CARD FRAUD

CARD FRAUD LOSSES SPLIT BY TYPE (AS PERCENTAGE OF TOTAL LOSSES)

- Lost/stolen
- Mail non-receipt
- Counterfeit
- Card-not-present
- Card ID theft

![2001 Data](chart)

- Lost/stolen: 28%
- Mail non-receipt: 7%
- Counterfeit: 3%
- Card-not-present: 11%
- Card ID theft: 4%

![2011 Data](chart)

- Lost/stolen: 7%
- Mail non-receipt: 3%
- Counterfeit: 15%
- Card-not-present: 65%
- Card ID theft: 11%
**FRAUD LOSSES ON UK-ISSUED CARDS SPLIT BY UK REGION 2007-2011**

All figures in £ millions

<table>
<thead>
<tr>
<th>Region</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>+/- change 10/11</th>
</tr>
</thead>
<tbody>
<tr>
<td>South East</td>
<td>179.0</td>
<td>204.6</td>
<td>167.8</td>
<td>156.6</td>
<td>149.9</td>
<td>-4%</td>
</tr>
<tr>
<td>North West</td>
<td>35.6</td>
<td>42.4</td>
<td>39.0</td>
<td>23.5</td>
<td>21.1</td>
<td>-10%</td>
</tr>
<tr>
<td>West Midlands</td>
<td>24.4</td>
<td>23.5</td>
<td>22.4</td>
<td>16.5</td>
<td>14.2</td>
<td>-14%</td>
</tr>
<tr>
<td>Yorkshire &amp; Humberside</td>
<td>24.0</td>
<td>22.1</td>
<td>18.5</td>
<td>15.4</td>
<td>12.2</td>
<td>-21%</td>
</tr>
<tr>
<td>East Midlands</td>
<td>22.8</td>
<td>24.3</td>
<td>19.4</td>
<td>13.6</td>
<td>16.6</td>
<td>+22%</td>
</tr>
<tr>
<td>South West</td>
<td>11.8</td>
<td>19.2</td>
<td>13.0</td>
<td>13.4</td>
<td>10.3</td>
<td>-23%</td>
</tr>
<tr>
<td>Scotland</td>
<td>11.5</td>
<td>17.9</td>
<td>11.4</td>
<td>10.6</td>
<td>9.8</td>
<td>-8%</td>
</tr>
<tr>
<td>Wales</td>
<td>5.3</td>
<td>7.4</td>
<td>8.2</td>
<td>7.9</td>
<td>7.6</td>
<td>-4%</td>
</tr>
<tr>
<td>North East</td>
<td>7.7</td>
<td>10.0</td>
<td>10.1</td>
<td>7.8</td>
<td>4.8</td>
<td>-38%</td>
</tr>
<tr>
<td>East Anglia</td>
<td>4.8</td>
<td>7.6</td>
<td>6.1</td>
<td>5.4</td>
<td>8.1</td>
<td>+50%</td>
</tr>
<tr>
<td>Northern Ireland</td>
<td>0.7</td>
<td>0.7</td>
<td>1.4</td>
<td>0.8</td>
<td>6.3</td>
<td>+659%</td>
</tr>
<tr>
<td><strong>UK TOTAL</strong></td>
<td>327.6</td>
<td>379.7</td>
<td>317.4</td>
<td>271.5</td>
<td>261.0</td>
<td>-4%</td>
</tr>
<tr>
<td><strong>Fraud abroad</strong></td>
<td>207.6</td>
<td>230.1</td>
<td>122.6</td>
<td>93.9</td>
<td>80.0</td>
<td>-15%</td>
</tr>
<tr>
<td><strong>TOTAL ALL UK CARDS</strong></td>
<td>535.2</td>
<td>609.9</td>
<td>440.0</td>
<td>365.4</td>
<td>341.0</td>
<td>-7%</td>
</tr>
</tbody>
</table>

In Northern Ireland, East Anglia and East Midlands the increases may point to the fact that the head offices of some organisations that accept CNP transactions are located in these areas.
PLASTIC CARD FRAUD

PHONE, INTERNET AND MAIL ORDER (CARD-NOT-PRESENT OR CNP) FRAUD

£220.9 MILLION IN 2011 (DOWN 3%)

This crime most commonly involves the theft of genuine card details that are then used to make a purchase over the internet, by phone, or by mail order.

In general, the difficulty in countering this type of fraud lies in the fact that neither the card nor the cardholder is present when the transaction happens.

Card-not-present fraud accounts for 65 percent of all card fraud, but these losses have to be seen in the context of a massive growth in CNP spending over the past ten years, especially over the internet.

In light of this growth it is all the more impressive that CNP fraud has fallen for the third successive year.

The reasons behind the continued decrease include the increasing use of sophisticated fraud screening detection tools by retailers and banks, as well as the growth in the use of American Express SafeKey, MasterCard SecureCode and Verified by Visa by both online retailers and cardholders.

The industry’s Be Card Smart Online campaign, launched at the end of 2008, provides consumers with straightforward practical tips to help them shop safely on the internet.
CARD-NOT-PRESENT FRAUD LOSSES ON UK-ISSUED CARDS 2001-2011

Tinted figures show percentage change on previous year’s total

<table>
<thead>
<tr>
<th>Year</th>
<th>£ millions</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>95.7</td>
<td>+31%</td>
</tr>
<tr>
<td>2002</td>
<td>110.1</td>
<td>+15%</td>
</tr>
<tr>
<td>2003</td>
<td>122.1</td>
<td>+11%</td>
</tr>
<tr>
<td>2004</td>
<td>150.8</td>
<td>+24%</td>
</tr>
<tr>
<td>2005</td>
<td>183.2</td>
<td>+21%</td>
</tr>
<tr>
<td>2006</td>
<td>212.7</td>
<td>+16%</td>
</tr>
<tr>
<td>2007</td>
<td>290.5</td>
<td>+37%</td>
</tr>
<tr>
<td>2008</td>
<td>328.4</td>
<td>+13%</td>
</tr>
<tr>
<td>2009</td>
<td>266.4</td>
<td>-19%</td>
</tr>
<tr>
<td>2010</td>
<td>226.9</td>
<td>-15%</td>
</tr>
<tr>
<td>2011</td>
<td>220.9</td>
<td>-3%</td>
</tr>
</tbody>
</table>
14// PLASTIC CARD FRAUD
COUNTERFEIT CARD FRAUD

£36.1 MILLION IN 2011 (DOWN 24%)

Counterfeit card fraud occurs when a fake card is created by fraudsters using compromised details from the magnetic stripe of a genuine card. This type of fraud has fallen by 79 per cent in the past three years. There are several factors for this, including:

- More countries have now introduced chip and PIN technology, which makes it much harder to use fake UK cards overseas.
- Increasing use by card companies of sophisticated fraud prevention software.
- The banking industry working closely with the retail community to raise awareness of the ways in which retailers can protect their chip and PIN terminals from criminal attack – minimising the opportunities for card details to be electronically copied.
- The continuing rollout of debit and credit cards with enhanced security features. Cards with an updated integrated card verification value (iCVV) have been rolled out since January 2008 and as of the end of December 2011 there were more than 134 million issued in the UK. In addition issuers are also rolling out Dynamic Data Authentication (DDA) cards, which also prevents counterfeiting by making each transaction unique, and at the end of 2011 there were more than 98 million of these cards in circulation.
- The successful work of the banking industry-sponsored special police unit, the Dedicated Cheque and Plastic Crime Unit (DCPCU), which has prevented approximately £400 million in fraud losses in the past ten years.
PLASTIC CARD FRAUD

Counterfeit card fraud losses in the UK have decreased by 72 per cent since 2004 – this is due to the fact that chip and PIN has made it much harder for criminals to use fake cards in cash machines and shops in the UK.

COUNTERFEIT CARD FRAUD LOSSES IN THE UK AND ABROAD 2007-2011
All figures in £ millions

<table>
<thead>
<tr>
<th>Region</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>+/- change 10/11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domestic (in the UK)</td>
<td>31.0</td>
<td>36.2</td>
<td>24.5</td>
<td>16.8</td>
<td>15.6</td>
<td>-7%</td>
</tr>
<tr>
<td>Abroad</td>
<td>113.3</td>
<td>133.6</td>
<td>56.4</td>
<td>30.8</td>
<td>20.5</td>
<td>-33%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>144.3</td>
<td>169.8</td>
<td>80.9</td>
<td>47.6</td>
<td>36.1</td>
<td>-24%</td>
</tr>
</tbody>
</table>
COUNTERFEIT CARD FRAUD LOSSES ON UK-ISSUED CARDS 2001-2011

Tinted figures show percentage change on previous year’s total.
18// PLASTIC CARD FRAUD

LOST AND STOLEN CARD FRAUD
£50.1 MILLION IN 2011 (UP 13%)

This category covers fraud on cards that have been reported by the cardholder as lost or stolen. Lost and stolen cards can be used in shops that do not have chip and PIN, or to commit a fraudulent telephone, internet or mail order transaction. If the PIN is also obtained, the card could be used in a shop or cash machine.

Initiatives such as chip and PIN have made it harder to commit ‘high-tech’ frauds. Fraudsters are instead reverting to more basic frauds focused around stealing people’s cards and PINs. These scams range from distracting people in shops or at cash machines and then stealing their cards without them noticing (distraction thefts), to simply tricking them into handing over their cards and PINs on their own doorstep (often referred to as courier scams or telephone scams).

Banking industry initiatives in place to tackle this type of fraud include:
- Chip and PIN.
- Intelligent computer systems that card companies use to track customer accounts for unusual spending patterns.
- An Industry Hot Card File (IHCF) that enables retailers to check electronically whether a card has been reported lost or stolen.
LOST AND STOLEN FRAUD LOSSES ON UK-ISSUED CARDS 2001-2011

Tinted figures show percentage change on previous year’s total

£ millions

<table>
<thead>
<tr>
<th>Year</th>
<th>Amount</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>114.0</td>
<td>+12%</td>
</tr>
<tr>
<td>2002</td>
<td>108.3</td>
<td>-5%</td>
</tr>
<tr>
<td>2003</td>
<td>112.4</td>
<td>+4%</td>
</tr>
<tr>
<td>2004</td>
<td>114.4</td>
<td>+2%</td>
</tr>
<tr>
<td>2005</td>
<td>89.0</td>
<td>-22%</td>
</tr>
<tr>
<td>2006</td>
<td>68.5</td>
<td>-23%</td>
</tr>
<tr>
<td>2007</td>
<td>56.2</td>
<td>-18%</td>
</tr>
<tr>
<td>2008</td>
<td>54.1</td>
<td>-4%</td>
</tr>
<tr>
<td>2009</td>
<td>47.7</td>
<td>-7%</td>
</tr>
<tr>
<td>2010</td>
<td>44.4</td>
<td>-7%</td>
</tr>
<tr>
<td>2011</td>
<td>50.1</td>
<td>13%</td>
</tr>
</tbody>
</table>
CARD ID THEFT
£22.5 MILLION IN 2011 (DOWN 41%)
Card ID theft occurs when a criminal uses a fraudulently obtained card or card details, along with stolen personal information, to open or take over a card account held in someone else’s name.
This type of fraud is split into two categories: third-party application fraud and account takeover fraud.

APPLICATION FRAUD
£4.0 MILLION IN 2011 (DOWN 21%)
Application fraud occurs when criminals use stolen or fake documents to open an account in someone else’s name. For identification purposes, criminals may try to steal documents such as utility bills and bank statements to build up useful personal information. Alternatively, they may use counterfeit documents.

ACCOUNT TAKEOVER
£18.5 MILLION IN 2011 (DOWN 44%)
This involves a criminal fraudulently using another person’s credit or debit card account, first by gathering information about the intended victim, then contacting their bank or credit card issuer to masquerade as the genuine cardholder. The criminal will then arrange for funds to be transferred out of the account, or will change the address on the account and ask for new or replacement cards to be sent.
ID THEFT ON UK-ISSUED CARDS 2001-2011
Tinted figures show percentage change on previous year’s total

£ millions

<table>
<thead>
<tr>
<th>Year</th>
<th>Amount (£ millions)</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>14.6</td>
<td>-16%</td>
</tr>
<tr>
<td>2002</td>
<td>20.6</td>
<td>+41%</td>
</tr>
<tr>
<td>2003</td>
<td>30.2</td>
<td>+47%</td>
</tr>
<tr>
<td>2004</td>
<td>36.9</td>
<td>+22%</td>
</tr>
<tr>
<td>2005</td>
<td>30.5</td>
<td>-17%</td>
</tr>
<tr>
<td>2006</td>
<td>31.9</td>
<td>+5%</td>
</tr>
<tr>
<td>2007</td>
<td>34.1</td>
<td>+7%</td>
</tr>
<tr>
<td>2008</td>
<td>47.4</td>
<td>+39%</td>
</tr>
<tr>
<td>2009</td>
<td>38.2</td>
<td>-19%</td>
</tr>
<tr>
<td>2010</td>
<td>38.1</td>
<td>0%</td>
</tr>
<tr>
<td>2011</td>
<td>22.5</td>
<td>-41%</td>
</tr>
</tbody>
</table>
MAIL NON-RECEIPT FRAUD
£11.3 MILLION IN 2011 (UP 34%)

This type of fraud involves cards being stolen whilst in transit – after card companies send them out and before the genuine cardholders receive them. Properties with communal letterboxes, such as flats and student halls of residence, and people who do not get their mail redirected when they change address are all vulnerable to this type of fraud.

In 2011 a large number of cards were upgraded to include contactless technology. This increase in the number of cards being sent out to customers contributed to the rise in this type of fraud.

Although this type of fraud has risen, it is still 85 per cent lower than in 2004, which was the peak year for mail non-receipt fraud. The banking industry continues to work with the Royal Mail, and other organisations it uses to deliver its cards, to monitor card losses, identify fraud hot spots and take preventative action. Card companies use secure couriers to deliver to high-risk postcodes, or cards may be sent to a customer’s branch for personal collection. Customers may also be required to phone their card company to activate their card before it can be used.
MAIL NON-RECEIPT FRAUD LOSSES ON UK-ISSUED CARDS 2001-2011
Tinted figures show percentage change on previous year’s total

£ millions


26.8 +51% 37.1 +39% 45.1 +22% 72.9 +62% 40.0 -45% 15.4 -61% 10.2 -34% 10.2 0% 6.9 -32% 8.4 +22% 11.3 +34%
WHERE DOES CARD FRAUD TAKE PLACE?

The card fraud landscape has changed over the past ten years mainly due to the continuing success of chip and PIN in the UK. Fraudsters are now targeting those environments that do not yet use chip and PIN, such as the internet. Overseas fraud losses have also gone down from their peak in 2008, due in part to the continuing rollout of chip and PIN in other countries around the world.

UK RETAILER (FACE-TO-FACE) FRAUD
£43.2 MILLION IN 2011 (DOWN 36%)

Card fraud losses in the UK high street have declined by 80 per cent since peaking at £218.8 million in 2004. This decrease is thanks to the success of chip and PIN. However, card fraud can still happen in shops in the UK on lost and stolen cards if a criminal has access to the PIN, for example, if a cardholder has written their PIN down and stored it in their purse or wallet, which is then stolen.

Cards could also be used fraudulently as a result of mail non-receipt fraud, where the fraudster has been able to intercept both the card and its PIN on the way to the cardholder, or where a fraudster has taken over an account and ordered a new card and PIN.
CARD FRAUD LOSSES AT UK RETAILERS (FACE-TO-FACE TRANSACTIONS) 2001-2011

Tinted figures show percentage change on previous year’s total

<table>
<thead>
<tr>
<th>Year</th>
<th>Millions</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>188.9</td>
<td>+36%</td>
</tr>
<tr>
<td>2002</td>
<td>186.9</td>
<td>+1%</td>
</tr>
<tr>
<td>2003</td>
<td>177.9</td>
<td>-5%</td>
</tr>
<tr>
<td>2004</td>
<td>218.8</td>
<td>+23%</td>
</tr>
<tr>
<td>2005</td>
<td>135.9</td>
<td>-38%</td>
</tr>
<tr>
<td>2006</td>
<td>72.1</td>
<td>-47%</td>
</tr>
<tr>
<td>2007</td>
<td>73.0</td>
<td>+1%</td>
</tr>
<tr>
<td>2008</td>
<td>98.5</td>
<td>+35%</td>
</tr>
<tr>
<td>2009</td>
<td>71.8</td>
<td>-27%</td>
</tr>
<tr>
<td>2010</td>
<td>67.4</td>
<td>-6%</td>
</tr>
<tr>
<td>2011</td>
<td>43.2</td>
<td>-36%</td>
</tr>
</tbody>
</table>
UK CASH MACHINE FRAUD

£29.3 MILLION IN 2011 (DOWN 12%)

The amount of money withdrawn fraudulently last year at UK cash machines, on UK-issued cards accounted for nine per cent of total card fraud losses. A lot of cash machine fraud is still the result of cardholders keeping their PIN written down in their purse or wallet, which is then stolen.

Fraudsters also target cash machines in order to compromise or steal cards or card details. The three main ways in which cards and card details are stolen at cash machines are:

- Card-trapping devices – a device is inserted into a cash machine’s card slot, which retains the card inside the cash machine. The criminal tricks the victim into re-entering their PIN while the criminal watches. After the cardholder gives up and leaves, the criminal removes the device, with the card, and withdraws cash.

- Skimming – a device is attached to the cash machine to record the electronic details from the magnetic stripe of genuine cards as they are inserted. A miniature camera is hidden overlooking the PIN pad to capture the PIN being entered. A fake magnetic stripe card is then produced and used with the genuine PIN to withdraw cash at cash machines overseas, which have yet to be upgraded to chip and PIN.

- Shoulder surfing – criminals watch the cardholder entering their PIN, then steal the card using distraction techniques or pickpocketing, before using the stolen card and genuine PIN.
FRAUD LOSSES AT UK CASH MACHINES 2001-2011
Tinted figures show percentage change on previous year’s total

£ millions


21.2 +16% 29.1 +37% 41.1 +41% 74.6 +81% 65.8 -12% 62.0 -6% 35.0 -44% 45.7 +31% 36.7 -20% 33.2 -9% 29.3 -12%
FRAUD ABROAD

£80.0 MILLION IN 2011 (DOWN 15%)

This type of fraud typically occurs as a result of criminals stealing magnetic stripe details from UK cards to make fake magnetic stripe cards for use overseas in countries yet to upgrade to chip and PIN. At £80 million, fraud abroad accounts for just under one quarter (23 per cent) of total card fraud losses. This type of fraud has dropped significantly in the past three years, partly due to banks’ fraud detection systems, which monitor for unusual spending patterns and stop potential fraud before it happens.

The countries where fraud is occurring on UK-issued cards have also changed markedly over the past five years. As chip and PIN is rolled out in more and more locations around the world, fraudsters are focusing on countries without chip and PIN, such as the USA, where they can still use fake magnetic stripe cards.
FRAUD COMMITTED ABROAD ON UK-ISSUED CARDS 2001-2011
Tinted figures show percentage change on previous year’s total
TOP 5 COUNTRIES FOR FRAUD ABROAD 2008-2011
UK-issued cards or card details used fraudulently overseas
INTERNET/E-COMMERCE FRAUD ON CARDS
ESTIMATED AT £139.6 MILLION IN 2011 (UP 3%)

An estimated £139.6 million of card fraud took place over the internet in 2011, an increase of 3 per cent from 2010 when e-commerce fraud losses were £135.1 million. Internet fraud now accounts for 63 per cent of card-not-present losses – slightly up from 59 per cent in 2010.

The fight against internet fraud has been aided by the increasing use of sophisticated fraud screening detection tools by retailers and banks to detect potential internet fraud, as well as the continued growth in use of American Express SafeKey, MasterCard SecureCode and Verified by Visa.

The vast majority of this type of fraud involves the use of card details that have been fraudulently obtained through methods such as skimming, hacking into retailers’ data connections, or through unsolicited emails or telephone calls. The card details are then used to undertake fraudulent card-not-present transactions.
INTERNET / E-COMMERCE FRAUD LOSSES ON UK-ISSUED CARDS 2001-2011
Tinted figures show percentage change on previous year’s total. All figures estimated.
INDUSTRY MEASURES TO PREVENT PLASTIC CARD FRAUD

CHIP AND PIN ________________________
MAKING CARD TRANSACTIONS SAFER

Chip and PIN is part of a global programme to tackle plastic card fraud and has proven to be an undoubted success, resulting in significant reductions in specific types of fraud on UK cards:
- Counterfeit card fraud is at its lowest level since 1998.
- Fraud losses in the UK high street have fallen by 80 per cent since 2004.
DEDICATED CHEQUE AND PLASTIC CRIME UNIT (DCPCU)

A SPECIALIST POLICE UNIT TARGETING ORGANISED CRIMINAL GANGS

The DCPCU is a specialist police unit fully sponsored by the banking industry, with an ongoing brief to help stamp out organised payment fraud across the UK. Uniquely it comprises officers from the Metropolitan and City of London police forces who work alongside banking industry fraud investigators and support staff.

The Unit has been responsible for estimated savings of approximately £400 million since its launch in 2002.

FINANCIAL FRAUD BUREAU (FFB)

The FFB is responsible for managing the payment industry’s co-ordinated initiatives on data sharing to reduce financial fraud. The Bureau is recognised as a centre of excellence and enables its customer groups to share data through a secure and trusted process. It provides data directly to law enforcement, including the DCPCU and the National Fraud Intelligence Bureau.

It is responsible for supporting and co-ordinating the Payments Industry Threat Management Process and maintaining the Fraud Intelligence Sharing System (FISS) database. It also issues and receives intelligence alerts from the payments industry and a wide range of other stakeholders.
FRAUD INTELLIGENCE SHARING SYSTEM (FISS)

SHARING INTELLIGENCE TO TACKLE FRAUD

FISS was established in 2008, and enables the banking industry to share information on all confirmed, attempted and suspected fraud in a central, shared database. Established specifically to combat all types of banking-related fraud in the UK, the system provides the industry with a secure and robust reporting mechanism, supporting the industry’s long-term fraud prevention strategy.

NATIONAL FRAUD AUTHORITY (NFA)

The industry works closely with the NFA through a series of coordinated fraud prevention activities, focused at key segments of society particularly at risk of financial fraud.

FIGHTING FRAUD TOGETHER

Thirty-seven organisations including The UK Cards Association and FFA UK have joined forces to launch ’Fighting Fraud Together’, a new strategy that aims to reduce fraud. It is the first time that the government, industry representatives, voluntary groups and law enforcement agencies have joined together on such a large scale to sign a joint commitment to tackle fraud.

NATIONAL FRAUD INTELLIGENCE BUREAU (NFIB)

The payments industry has worked closely with the City of London Police to establish the NFIB and now provides a regular data feed from FISS. The NFIB is one of the most advanced police intelligence systems in the world, using millions
of reports of fraud from a wide range of public and private sector organisations to help catch serial fraudsters and provide a better picture of the nature of fraud.

The Bureau is government-funded and run by the City of London Police, which is the National Lead Force for fraud, in partnership with police forces and the public and private sector.

**INDUSTRY HOT CARD FILE (IHCF)**

**CHECKING TRANSACTIONS FOR CARDS BEING USED FRAUDULENTLY**

The IHCF contains information on more than six million cards reported lost or stolen. In 2011, 463,000 (425,000 in 2010) cases of attempted fraud were prevented by this system. The IHCF is also used successfully at French motorway tollbooths to combat the use of stolen UK cards.

More than 60,000 UK retailers subscribe to this electronic file. When a participating retailer accepts a card payment as part of a normal transaction, it is automatically checked against the file, and the retailer is alerted if the card’s details match any of those on the system.

The IHCF is increasingly used by retailers in the card-not-present environment, providing a mechanism for checking card details prior to goods being dispatched.
REDUCING PHONE, INTERNET AND MAIL ORDER (CARD-NOT-PRESENT) FRAUD

HELPING BUSINESSES FIGHT CNP FRAUD

Phone, internet and mail order fraud fell for the third successive year in 2011 although these losses still account for more than half of all card fraud. However, the fall in this type of fraud is all the more notable given the continuing popularity of shopping over the phone and the internet. The estimated total value of internet spending in 2011 was £63.2 billion – an increase of 18 per cent on the previous year (£53.6 billion in 2010).

A number of initiatives are in place to tackle phone, internet and mail order fraud:

- American Express SafeKey, MasterCard SecureCode and Verified by Visa are online fraud prevention initiatives that make cards more secure when shopping online by adding an extra layer of protection. Cardholders simply register their card when prompted and create a password that they will be asked to provide at participating retailers. More than half of all cards issued in the UK have been registered to date.

- More information can be found at www.financialfraudaction.org.uk as well as via your bank or card company.
- An automated cardholder address verification (AVS) and card security code (CSC) system is available for businesses that accept phone, internet or mail order transactions. The system allows them to verify the billing address of a cardholder and cross-check the security code on the signature strip of the card. These data checks provide additional information to help businesses assess fraud risks and decide whether to proceed with the transaction.

- The industry encourages retailers to make use of American Express SafeKey, MasterCard SecureCode and Verified by Visa, as well as various card-not-present fraud prevention tools, such as intelligent fraud detection software, available from third-party providers.
BANKS’ USE OF INTELLIGENT FRAUD-DETECTION SYSTEMS
CHECKING FOR UNUSUAL SPENDING PATTERNS TO SPOT FRAUD BEFORE IT IS REPORTED BY THE CARDHOLDER

Card companies continue to increase the effectiveness and sophistication of customer-profiling neural networks that can identify unusual spending patterns and potentially fraudulent transactions. The card company will then contact the cardholder to check whether the suspect transaction is genuine. If not, an immediate block can be put on the card.

INDUSTRY MEASURES TO PREVENT CARD ID THEFT
CROSS-INDUSTRY CO-OPERATION

Card ID fraud continues to be a relatively small proportion of total card fraud losses – just over six per cent – but the industry remains committed to enhancing existing prevention measures and developing new ways of combating this type of fraud.

The banking industry has created a website for identity fraud prevention at www.identitytheft.org.uk, which provides best practice guidelines for businesses that could be targeted by identity fraudsters. There is also an interactive e-learning section to help employees who check and verify the identity of customers on a day-to-day basis.
The site also advises the public how best to protect themselves from becoming a victim of identity theft and what to do if they have. This is complemented with a range of leaflets and posters for use in public areas such as libraries, Citizens Advice Bureaux and bank counters.

For more information visit www.identitytheft.org.uk.

INDUSTRY MEASURES TO PREVENT CASH MACHINE CRIME

MULTI-LAYERED APPROACH TO TACKLING FRAUD

Although UK cash machine fraud losses have decreased by 61 per cent since 2004 – the peak year for this type of fraud – the UK banking industry continues to work with cash machine suppliers to enhance technical solutions to prevent cash machine tampering. The industry also works with the police to target the organised criminals behind these types of crime.
A number of generic initiatives are in place to counter cash machine crime. These include:

- Technology upgrades to make cash machines tamper-proof, such as redesigned card reader surrounds in order to make it difficult for fraudsters to attach a magnetic stripe reader to a machine.

- Encouraging regular inspections of cash machines by cash machine owners for evidence of tampering and unusual attachments.

- Use of CCTV to deter criminal activity.

- Consumer advice on best practice when using a cash machine. This includes co-ordinating use of screen messages designed to raise security awareness.

- LINK, the UK’s cash machine network, also works in partnership with independent charity Crimestoppers, to offer rewards of up to £25,000 for information on cash machine crime. Anyone with details about those responsible for any type of cash machine crime can call Crimestoppers on 0800 555 111, where they can leave their information anonymously.
PLASTIC CARD FRAUD
CHEQUE FRAUD

£34.3 MILLION IN 2011 (UP 17%)
Following year-on-year decreases since 2007, last year saw a 17 per cent increase in cheque fraud losses. The main reason for this rise is an increase in fraudsters stealing genuine cheques and altering the payee name, or using details from genuine cheques to create counterfeits.

There are three types of cheque fraud: counterfeit, forged, and fraudulently altered cheques.

TYPES OF CHEQUE FRAUD

// COUNTERFEIT CHEQUE FRAUD
£7.8 MILLION IN 2011 (UP 109%)
Counterfeit cheques are printed on non-bank paper to look exactly like genuine cheques and are drawn by a fraudster on genuine accounts.

// FORGED CHEQUE FRAUD
£14.4 MILLION IN 2011 (UP 6%)
A forged cheque is a genuine cheque that has been stolen from an innocent customer and used by a fraudster with a forged signature.

// FRAUDULENTLY ALTERED CHEQUES
£12.1 MILLION IN 2011 (UP 1%)
A fraudulently altered cheque is a genuine cheque that has been made out by the genuine customer, but a fraudster has altered the cheque in some way before it is paid in, e.g. by altering the beneficiary’s name or the amount of the cheque.
## Cheque Fraud Losses 2002-2011

Tinted figures show percentage change on previous year’s total

<table>
<thead>
<tr>
<th>Year</th>
<th>Losses (£ millions)</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>36.0</td>
<td></td>
</tr>
<tr>
<td>2003</td>
<td>45.0 (+25%)</td>
<td></td>
</tr>
<tr>
<td>2004</td>
<td>46.2 (+3%)</td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td>40.3 (-13%)</td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td>30.6 (-24%)</td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>33.5 (+10%)</td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>41.9 (+25%)</td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td>29.8 (-29%)</td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td>29.3 (-1%)</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>34.3 (+17%)</td>
<td></td>
</tr>
</tbody>
</table>
COMMON CHEQUE SCAMS

There are a number of cheque scams. They may involve not only stolen or fraudulent cheques and bankers’ drafts, but also genuine cheques owned by the fraudster, which bounce due to lack of sufficient funds.

In recent years organised gangs have targeted consumers selling high-value goods such as cars, offering stolen or counterfeit cheques and bankers’ drafts. Anyone accepting a cheque or banker’s draft is advised not to hand over the goods until they have certainty that the cheque funds will not be reclaimed (this happens at the end of the sixth working day after they have paid the cheque into their account). Frequently the fraudster will offer a cheque or banker’s draft for significantly more than the price of the goods. As ever, anything that sounds too good to be true should set alarm bells ringing, even if the fraudster’s excuse sounds plausible.

The seller is asked to transfer the amount of the overpayment either to the fraudster, or a third party after three days when, it is claimed, the cheque will be cleared. Banks do all they can to spot and stop such cheques and drafts in the clearing system. However, with this scam, the cheque might be genuine, but the fraudster does not have sufficient funds in their account. The paying bank will therefore return the cheque unpaid. If the customer has already made the overpayment to a third party, they will lose the funds. With the 2-4-6 clearing timescales it is not until the end of the sixth working day after the cheque has been paid
in that the customer can be sure that the funds are theirs, and will not bounce (see 2-4-6 clearing timescales on next page).

Another type of cheque scam involves fraudsters altering a genuine cheque to add an extra name to the payee line – without any of the original detail being removed. Fraudsters target cheques where there is an unused space in the payee line, by adding ‘re’, ‘or’, ‘T/As’ or ‘c/o’ followed by a new name in the space left blank. This type of fraud means there are no signs of obvious alteration, reinforcing the importance of drawing a line through all unused spaces when writing out a cheque. It is also important when writing a cheque to an individual, a business or an organisation to write their name in full, using a black or blue ballpoint or a pen with indelible ink to prevent a fraudster making an alteration to the original details, or opening an account in the beneficiary’s name so that they can pay in the cheque and withdraw the funds.
WHAT IS THE BANKING INDUSTRY DOING TO PROTECT CUSTOMERS FROM CHEQUE FRAUD?

The banking industry introduced the 2-4-6 cheque clearing timescales to help protect customers who inadvertently accept cheques from fraudsters. It means that customers can be sure that at the end of six working days after paying in a cheque the money is theirs. Should the cheque subsequently turn out to be fraudulent the customer is protected from any loss and the funds cannot be reclaimed without the customer’s consent unless the customer is a knowing party to fraud.

Despite this positive change, the industry continues to recommend that customers should be wary of accepting cheques or bankers’ drafts if they don’t know or trust the person offering them – particularly if they are of high value.
WHAT IS THE BANKING INDUSTRY DOING TO PREVENT CHEQUE FRAUD?

There is a range of prevention measures employed at both bank and industry level. At an industry level, banks continue to focus on identifying lost, stolen or fraudulent cheques as they pass through the clearing system, before there is a victim. In the past year the banking industry successfully identified over 90 per cent of all fraudulent cheques as they went through the cheque clearing process.

Another way in which the industry is combating cheque fraud is through the Cheque Printer Accreditation Scheme (CPAS), which was set up in 1995 and is managed by the Cheque and Credit Clearing Company. All printers of cheques are required to be accredited to the Scheme, and to comply with the regulations for ensuring that cheques are printed to the highest security standards. Customers’ chequebooks are printed by CPAS members.
LIABILITY FOR CHEQUE FRAUD

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.

Following the introduction of the 2-4-6 cheque changes, a customer accepting a cheque can be sure that at the end of six working days (after paying a cheque or banker’s draft into their bank account) the money is theirs.

They are protected from any loss, should the cheque turn out to be fraudulent – the funds cannot be reclaimed without the customer’s consent unless the customer is a knowing party to fraud. However, any customers who do not wait until the end of the sixth working day, and decide to withdraw and spend funds before that, do so at their own risk.

If the cheque subsequently bounces, they may have to return funds to their bank or building society.
ONLINE AND PHONE BANKING FRAUD

ONLINE BANKING FRAUD

INDUSTRY MEASURES TO PREVENT ONLINE BANKING FRAUD

PHONE BANKING FRAUD
In 2011 online banking fraud losses totalled £35.4 million – a decrease of 24 per cent from the previous year (£46.7 million in 2010).

The reduction in online banking fraud is due to a number of factors. Although more customers are now banking online, customers have become more aware of security and have become better at securing their PCs. Other factors include banks’ increasing use of sophisticated fraud detection software to monitor and spot suspected fraudulent transactions as well as banks providing customers with additional software and hand-held devices to log on to internet banking.

The Police Central e-Crime Unit (PCEU), is also helping to tackle these losses by providing specialist police officer training and co-ordinating cross-force initiatives to crack down on online criminals.
ONLINE BANKING FRAUD LOSSES 2004-2011
Tinted figures show percentage change on previous year’s total
COMMON SCAMS

PHISHING
Phishing describes the practice of sending emails at random, purporting to come from a genuine company such as a bank, in an attempt to trick customers of that company into disclosing information at a bogus company website operated by fraudsters.

These emails usually claim that it is necessary to ‘update’ or ‘verify’ your password, and they urge you to click on a link from the email that takes you to the bogus bank website. Alternately, some phishing emails may ask you to enter your details on a form attached to the email. Any information entered on the bogus website or form will be captured by the criminals for their own fraudulent purposes.

Criminals use phishing because the banks’ own systems have proven difficult to attack. Criminals have focused their attention on phishing attacks, targeting individual internet users in order to gain personal or secret information that can be used online for fraudulent purposes.

MALWARE (MALICIOUS SOFTWARE)
Malware remains a popular method used by fraudsters to obtain customers’ details, and is sometimes used in combination with phishing emails.

Malware includes computer viruses that can be installed on a computer without the user’s knowledge, typically by clicking on a link in an unsolicited email, or by downloading infected software.

Malware is capable of inserting bogus web pages, logging keystrokes and performing unauthorised actions on your computer, in an attempt to capture passwords, financial information or other personal details.
### NUMBER OF PHISHING WEBSITES* TARGETED AGAINST UK BANKS AND BUILDING SOCIETIES BY MONTH 2005-2011

<table>
<thead>
<tr>
<th>Year</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
<th>June</th>
<th>July</th>
<th>Aug</th>
<th>Sept</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>5,803</td>
<td>5,757</td>
<td>6,828</td>
<td>5,698</td>
<td>6,216</td>
<td>6,896</td>
<td>7,402</td>
<td>8,062</td>
<td>23,083</td>
<td>9,397</td>
<td>15,395</td>
<td>10,749</td>
<td>111,286</td>
</tr>
<tr>
<td>2010</td>
<td>2,654</td>
<td>3,135</td>
<td>4,810</td>
<td>4,335</td>
<td>5,406</td>
<td>5,277</td>
<td>5,873</td>
<td>5,861</td>
<td>5,689</td>
<td>6,977</td>
<td>4,552</td>
<td>7,304</td>
<td>61,873</td>
</tr>
<tr>
<td>2009</td>
<td>4,206</td>
<td>5,161</td>
<td>5,004</td>
<td>3,422</td>
<td>3,917</td>
<td>4,335</td>
<td>4,415</td>
<td>4,845</td>
<td>3,900</td>
<td>4,903</td>
<td>4,191</td>
<td>5,864</td>
<td>51,161</td>
</tr>
<tr>
<td>2008</td>
<td>3,144</td>
<td>3,243</td>
<td>3,848</td>
<td>3,719</td>
<td>3,091</td>
<td>3,637</td>
<td>3,584</td>
<td>3,716</td>
<td>4,121</td>
<td>4,536</td>
<td>3,896</td>
<td>3,456</td>
<td>43,991</td>
</tr>
<tr>
<td>2007</td>
<td>1,290</td>
<td>974</td>
<td>1,130</td>
<td>1,188</td>
<td>1,274</td>
<td>1,368</td>
<td>3,066</td>
<td>3,268</td>
<td>2,597</td>
<td>3,170</td>
<td>3,277</td>
<td>3,195</td>
<td>25,797</td>
</tr>
<tr>
<td>2006</td>
<td>606</td>
<td>669</td>
<td>1,074</td>
<td>947</td>
<td>919</td>
<td>872</td>
<td>970</td>
<td>1,484</td>
<td>1,513</td>
<td>1,596</td>
<td>1,993</td>
<td>1,513</td>
<td>14,156</td>
</tr>
<tr>
<td>2005</td>
<td>18</td>
<td>29</td>
<td>27</td>
<td>54</td>
<td>72</td>
<td>122</td>
<td>153</td>
<td>160</td>
<td>190</td>
<td>267</td>
<td>255</td>
<td>353</td>
<td>1,700</td>
</tr>
</tbody>
</table>

* Fraudsters set up a website that is a fake version of a genuine bank website, and then send out thousands or even millions of spam emails trying to convince people to click on a link that will send them to that fake site.
MONEY MULES

Most fraudsters behind online banking scams are located overseas, so they need an accomplice with a UK bank account to act as a ‘money mule’ or money transfer agent, to launder the stolen funds. Some mules are recruited under false pretences, after applying for a job as a ‘payment processing agent’, in the belief that they will be working for a legitimate company.

After being recruited by the fraudsters, money mules receive funds into their accounts. They then withdraw the money and send it overseas using a wire transfer service, minus a percentage commission payment.

Money mules are recruited by a variety of methods, including spam emails, adverts on genuine recruitment websites or newspapers, and approaches to people with their CVs displayed online.

Although the prospect of making some easy money may appear attractive, any commission payments will be recovered as they are the proceeds of fraud, and money mules may become embroiled in a police investigation. Money mules are the easiest part of the chain to track down.
INDUSTRY MEASURES TO PREVENT ONLINE AND TELEPHONE BANKING FRAUD

As well as introducing additional security measures such as two-factor authentication and free security software for customers, the banking industry works with a number of partners, including the Serious Organised Crime Agency (SOCA), the Police Central e-Crime Unit (PCeU), overseas law enforcement agencies, technology companies, anti-virus firms and Internet Service Providers. The industry has also worked with the National Fraud Authority and others, on joint awareness campaigns to raise awareness of various types of online fraud and provide helpful security advice to consumers.

A number of initiatives are in place:
- Monitoring the internet at industry and bank level to detect and close down phishing-related websites;
- Two-way communication with online partners to share security intelligence; and
- Development and use of clear and consistent advice for consumers.

Some banks have provided customers with two-factor authentication devices. These can be a hand-held chip and PIN card reading device and work by a customer inserting their debit or credit card into the reader.
and entering their PIN. On confirming the PIN, the device generates a unique, one-time only passcode, which the cardholder provides when prompted to access their online account or make payments.

The industry also provides fraud prevention advice at www.banksafeonline.org.uk to help online banking users stay safe online.

PHONE BANKING FRAUD

£16.7 MILLION IN 2011 (UP 32%)

2009 was the first year that phone banking fraud losses were collated centrally – previously these figures were only quantified by banks on an individual basis. Producing an industry-wide figure will enable the industry to understand and help prevent this crime.
HOW DOES PHONE BANKING FRAUD HAPPEN?
This fraud happens when a criminal fraudulently accesses the victim’s phone banking account. To do this the criminal needs to be in possession of specific personal and financial information about the victim, to convince the phone banking system/operator that they are the genuine account holder. A criminal will use a variety of ways to acquire information about an intended victim such as social engineering, phishing, cold-calling (pretending to be from a bank or the police) and bin-raiding.

WHAT IS THE INDUSTRY DOING TO TACKLE THIS TYPE OF FRAUD?
All banks use sophisticated security systems to protect their customers’ accounts. These systems are constantly upgraded to maintain their effectiveness. Collectively, the banking industry shares information and intelligence with law enforcement and the telecommunications industry: to identify fraudulent activity and those seeking to undertake it, and to maintain the security of telephone-based services.
ONLINE AND PHONE BANKING FRAUD
Cards are a very safe way to pay for goods and services in the UK and overseas. If you are unlucky enough to become a victim of fraud the good news is that you are protected by legislation and should not suffer any financial loss – provided you have not acted fraudulently or without reasonable care.

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, and don’t leave your cards unattended in public places.
- Check receipts against statements regularly and contact your card company as soon as possible if you find an unfamiliar transaction.
- 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.
- Your bank or the police will NEVER ring you and tell you that they are coming to your home to pick up your card, so never hand it over to anyone who comes to collect it.
- Your bank will NEVER ask you to authorise anything by entering your PIN into the telephone.
- NEVER share your PIN with anyone – the only times you should use your PIN is at a cash machine or in a shop.
Keep it secret, keep it safe – protect your PIN
- Ensure you are the only person that knows your PIN. Your bank or the police will never phone you and ask you to disclose it; anyone who does ask you for your PIN is a fraudster.
- When entering your PIN, use your free hand and your body to shield the number, in case fraudsters have installed a hidden camera or are watching you over your shoulder. If you think someone has seen your PIN you can change it at a cash machine or by contacting your bank.

// USING YOUR CARDS OVERSEAS
Before you go overseas:
- Only take cards that you intend to use; leave others in a secure place at home.
- It’s a good idea to take another card or alternative payment method with you so that you are not reliant on just one card.
- Make sure you have your card company’s 24-hour contact telephone number.
- Make sure your card company has up-to-date contact details for you, including a mobile telephone number.
- If your cards are registered with a Card Protection Agency, ensure you have their contact telephone number and your policy number with you.

When you are overseas:
- Don’t let your card out of your sight, especially in restaurants and bars.
- Don’t give your PIN to anyone – even if they claim to be from the police or your card company.
ADVICE AND CONTACTS

- 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.

// CASH MACHINE FRAUD PREVENTION
Cash machines are generally very safe, however they do sometimes attract criminal attention so you still need to follow common sense precautions when withdrawing cash.

To minimise the chances of having your card or card details stolen at a cash machine:
- If you spot anything unusual about the cash machine, or there are signs of tampering, do not use it. Report it to the police immediately.
- Be alert and put your personal safety first. 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 free 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 it immediately to your card company, ideally
using your mobile phone while you are still in front of the machine. Destroy or preferably shred your cash machine receipts, mini-statements or balance enquiries when you dispose of them.

**AVOIDING CHEQUE FRAUD**
- Never accept a cheque, or banker’s draft from someone, unless you know and trust them. Be especially wary when accepting a high-value cheque; for instance if you are selling a car.
- Be aware that, until a cheque has been cleared at the end of the sixth working day after you have paid it in to your account, there is a risk that the money could be reclaimed if the cheque turns out to be stolen, fraudulently altered or counterfeited. It is safer to ask for payment for high-value items to be made by other means (an internet or phone banking payment or a CHAPS payment). There is a charge for a CHAPS payment but it is a guaranteed same-day value payment. However, most transaction will be below the Faster Payment limit of £10k, and will therefore be free.
- Be aware that a banker’s draft or building society cheque is not safe from fraud. Like a cheque if they are stolen, altered or are counterfeited they will not be honoured. If you receive a banker’s draft in payment for goods, you should wait until you have certainty at the end of the sixth working day after you’ve paid the draft in to your account before releasing the goods.
- Keep your chequebook in a safe place, report any missing cheques to your bank immediately and always check your bank statement thoroughly.
- Ensure every ‘space’ that is left blank on your cheque is crossed through i.e. after the amount in words and after the payee name.
- Always use a black or blue ballpoint or a pen with indelible ink.
- If you are making a cheque payable to a bank or credit card company to pay off your credit card bill, you must ensure that you provide sufficient details about the payee and enter the full details for the account holder in the payee line.

ONLINE FRAUD PREVENTION

ONLINE SHOPPING
- Sign up to American Express SafeKey, MasterCard SecureCode or Verified by Visa whenever you are given the option whilst shopping online. This involves you registering a password with your card company. By signing up, your card will have an additional level of security that will minimise the chances of you becoming a victim of online fraud.
- Only shop on secure sites. Before entering card details ensure that the locked padlock or unbroken key symbol is showing in your browser. Additionally, the beginning of the online retailer’s internet address will change from ‘http’ to ‘https’ to indicate the connection is secure.
- Never send your PIN over the internet.
- Keep a copy 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).
- Always log out properly after shopping online – if the website you have used has a ‘sign out’ or ‘log off’ button, click it when you have finished, especially if you have been using a shared or public computer.

More detailed advice on how to stay safe when shopping online is available at www.financialfraudaction.org.uk

// PHONE AND ONLINE BANKING
To help avoid scams you should:
- Always be suspicious of emails that are supposedly from your bank or from another bank that you do not deal with.
- Make sure your computer has up-to-date anti-virus software and a firewall installed; consider using browser security software. Some banks provide their customers with these tools free of charge.
- Download the latest security updates, known as patches, for your browser and for your operating system (e.g. Windows).
- Be wary of unsolicited requests for personal or financial information. Keep your passwords and PINs safe; your bank or the police would never contact you to ask you to disclose your PIN or password.
- If you are unsure, contact your bank direct over the phone using a number on your bank statement or on the back of your card.
As additional preventative measures when banking online, you are encouraged to:
- 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.
- Be particularly security-conscious if you are using a public computer or public Wi-Fi internet connection.
- 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, as the email could be fraudulent.

// IDENTITY THEFT
The following tips will help you protect your identity and prevent criminals from committing fraud in your name.
- Always keep important personal documents, plastic cards and chequebooks in a safe and secure place.
- Don’t share personal information unless you are confident you know who you are dealing with.
- When disposing of statements, receipts and documents that contain information relating to your financial affairs destroy them, preferably by shredding.
- Thoroughly check bank and card statements as soon as they arrive. 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 any other financial information contact the supplier as soon as possible.
- Get your post immediately redirected to your new address if you move house.
- More tips and advice are available from www.identitytheft.org.uk
- Be aware of security settings when using social networking sites.
- Never share your personal data (such as your date of birth or full address) on social networking sites or social media.

---

**IF YOU BECOME A VICTIM OF FRAUD**

Steps to take if you find you are a victim of fraud:

- If the fraud involves credit or debit cards, phone/online banking or cheques, you should report it to the financial institution concerned. They are responsible for undertaking further investigation and, as appropriate, reporting cases of criminal activity to the police.
- Any fraud that doesn’t involve your bank or card company should be reported to the business or organisations concerned in the first instance, and, dependent on their advice, to Action Fraud (the national fraud reporting centre).
- If an additional crime has been committed alongside the fraud, for example, you have had your wallet or purse stolen or the card
was stolen as a part of a burglary, then this should still be reported to the police.
- Ensure you keep a record of all communications.
- Get a copy of your personal credit report from one of the credit reference agencies – Call Credit, Equifax and Experian. A paper version of your report is available for a nominal fee. If applications for credit have been made in your name you can ask to have any incorrect information removed.
- 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 address. Over 260 credit businesses are CIFAS members. www.cifas.org.uk
- If you suspect mail theft, contact the Royal Mail customer enquiry number on 08456 740740 or visit www.royalmail.com
- If you are a victim of card fraud or online banking fraud you have protection through legislation, which states that you will not be liable for any losses unless you have acted fraudulently or without reasonable care.

Emergency contacts and advice is available at www.financialfraudaction.org.uk.
INDUSTRY CONTACTS

Financial Fraud Action UK
Working together to prevent fraud
www.financialfraudaction.org.uk
Financial Fraud Action UK is the name under which the financial services industry co-ordinates its activity on fraud, presenting a united front against financial fraud and its effects.

The UK Cards Association
www.theukcardsassociation.org.uk
The UK Cards Association is the leading trade association for the card payments industry in the UK.

Cheque & Credit Clearing Company
www.chequeandcredit.co.uk
The Cheque and Credit Clearing Company is a membership-based industry body which manages the cheque clearing system in Great Britain.

The strategic payments body set up to ensure that UK payment systems and services meet the needs of customers, payment service providers and the wider economy.
Identity Theft
Don’t become a victim

www.identitytheft.org.uk
How to help protect yourself or your business from identity theft, what to do if it happens to you and suggestions on where to get further help.

Bank Safe Online

www.banksafeonline.org.uk
Bank Safe Online is the UK banking industry’s initiative to help online banking customers stay safe online.

LINK

www.link.co.uk
LINK is the UK’s cash machine (ATM) network and the busiest ATM transaction switch in the world.

Pay Your Way

www.payyourway.org.uk
Pay Your Way is the Payments Council’s consumer awareness campaign, providing impartial information on different payment options.
PUBLICATIONS

// UK PAYMENT STATISTICS 2012
Provides a comprehensive source of UK payment statistics and historical data from 2001 to 2011, with additional forecast data up to and including 2020. £750.

// UK CASH AND CASH MACHINES 2012
Covers the main trends in cash payments, the deployment and usage of cash machines, and other forms of cash acquisition. £250.

// UK PLASTIC CARDS 2012
Plastic card trends in the UK by businesses and individuals. £250.

// UK AUTOMATED PAYMENTS 2012
Covers the main trends in the use of direct credits, Direct Debits, Faster Payments, standing orders and CHAPS payments. £250.
// UK CHEQUES 2012
Covers the main trends in the use of cheques for payment and cash acquisition. £250.

// UK CONSUMER PAYMENTS 2012
Looks in detail at consumer holdings and use of different payment methods. £1,500.

Please note that 2012 editions are currently in production. For more information or to order any of these publications please contact press@paymentscouncil.org.uk
ADVICE AND CONTACTS

OTHER USEFUL CONTACTS

PAYMENTS INDUSTRY PRESS OFFICE
(CHAPS, Cheque & Credit Clearing Company, DCPCU, Faster Payments, FFA UK, LINK, Payments Council, The UK Cards Association and SWIFT)
020 3217 8368
press@ukcards.org.uk
Sandra Quinn, Director of communications
020 3217 8234
M: 07768 044656
Jemma Smith, Head of PR
020 3217 8340
M: 07811 113075

Mark Bowerman, PR manager
020 3217 8251
M: 07799 627256
Michelle Whiteman, Press officer
020 3217 8316
Neil Aitken, Press officer
020 3217 8441
Doriena Koldenhof, PR assistant
020 3217 8368
Rosalind Beaumont, Public affairs manager
020 3217 8280
78 // ADVICE AND CONTACTS