FRAUD THE FACTS 2013

The definitive overview of payment industry fraud and measures to prevent it
FFA UK works closely with:
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 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 UK Cards Association (UKCA) 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
- Co-ordinates other industry-wide initiatives across matters relating to both card payments and the provision of credit

FFA UK is supported by:
The UK Cards Association (UKCA) 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
- Co-ordinates other industry-wide initiatives across matters relating to both card payments and the provision of credit

The Fraud Control Steering Group (FCSG) 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.

FCSG develops responses to technology and payments system innovation
- Delivers cross industry projects
- Ensures a unified industry fact-base through management information
- Delivers the Industry Hot Card File
- Provides Member relationship management as well as external relationship management
- Engages law enforcement and sponsors a dedicated Police Unit
- Informs the public (and media) through the use of education and awareness

Financial Fraud Action UK (FFA UK) leads the collective fight against fraud within the UK financial services industry. It works with industry partners and players for and on behalf of its Members. It:
- Ensures a unified voice on behalf of its Members
- Provides flexible and robust fraud and related financial crime intelligence sharing
- Manages an Industry Strategic Threat Management process

FFA UK works closely with:
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 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).
We remain incredibly proud of The UK Card Association’s close links with the fraud prevention community, particularly through our sponsorship of FFA UK and the Dedicated Cheque and Plastic Crime Unit (DCPCU). The integrated approach of FFA UK, which combines education and awareness, intelligence-sharing and law enforcement, continues to have a major impact in tackling organised fraud and in bringing both individual fraudsters and criminal gangs to justice.

In particular, the DCPCU celebrated its 10th anniversary in 2012, having provided an estimated £440 million of fraud savings to the industry since its inception.

GRAHAM PEACOP, Director of Cards and Fraud Control

2012 was a big year for the fraud prevention community, with major steps forward seen in the collaborative work we undertake with government to secure a step-change in the sharing of information on fraud. During 2012 we delivered a series of impactful awareness campaigns which were targeted at specific segments of the population known to be at greater risk of becoming fraud victims.

I am particularly pleased that we have been able to work so closely with our colleagues in the National Fraud Authority to deliver some of these initiatives.

KATY WOROBEC, Head of Fraud Control

www.financialfraudaction.org.uk
TRENDS AND STATISTICS

An overview of the different types of card fraud and a summary of card fraud trends
### Trends and Statistics

**Fraud losses on UK-issued cards 2002-2012**

Figures in white show percentage change on previous year’s total.

#### Annual fraud losses on UK-issued cards 2002-2012

<table>
<thead>
<tr>
<th>Fraud type</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>2012</th>
<th>+/- change 11/12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card-not present</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>245.8</td>
<td>+11%</td>
</tr>
<tr>
<td>Lost/stolen</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>55.2</td>
<td>-10%</td>
</tr>
<tr>
<td>Card ID theft</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>12.8</td>
<td>-13%</td>
</tr>
<tr>
<td>TOTAL</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>535.2</td>
<td>460.9</td>
<td>365.4</td>
<td>340.1</td>
<td>388.0</td>
</tr>
<tr>
<td>UK</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>286.7</td>
<td>+10%</td>
</tr>
<tr>
<td>Fraud abroad</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>101.3</td>
<td>+27%</td>
</tr>
</tbody>
</table>

Due to the rounding of figures, the sum of separate items may differ from the totals shown. E-commerce figures are estimated.
OVERVIEW OF CARD FRAUD LOSSES

Total fraud losses on UK cards increased by 14 per cent between 2011 and 2012 to £388 million. Card fraud losses against total turnover increased to 0.07 per cent, up 16 per cent on 2011. This follows three years of significant decreases since fraud was £610 million at its peak in 2008, representing an overall decrease of 36 per cent.

A return amongst criminals to traditional methods of fraud, such as low-tech deception crimes, has led to the increased fraud losses borne by the banking industry. The impact of improved security features, such as Chip & PIN and more sophisticated detection tools, has driven criminals to resort to deceiving consumers into such things as parting with their own cards, PINs and financial passwords.
Card fraud losses split by type (as percentage of total losses)

<table>
<thead>
<tr>
<th>Type</th>
<th>2002</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lost/stolen card</td>
<td>26%</td>
<td>6%</td>
</tr>
<tr>
<td>Mail non-receipt</td>
<td>5%</td>
<td>14%</td>
</tr>
<tr>
<td>Counterfeit card</td>
<td>26%</td>
<td>3%</td>
</tr>
<tr>
<td>Card-not-present</td>
<td>35%</td>
<td>11%</td>
</tr>
<tr>
<td>Card ID theft</td>
<td>9%</td>
<td>1%</td>
</tr>
</tbody>
</table>

TRENDS AND STATISTICS
PHOTO, INTERNET AND MAIL ORDER (CARD-NOT-PRESENT OR CNP) FRAUD

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 purchases over the Internet, 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 at the merchant when the transaction happens.

CNP fraud accounts for 63 per cent 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 and with the growth in remote shopping via mobile devices and tablets which is set to continue.
INTERNET/E-COMMERCE FRAUD ON CARDS

These fraud figures are included within the overall CNP fraud losses described in the previous section. An estimated £140.2 million of e-commerce fraud took place on cards in 2012, accounting for 36 per cent of all card fraud, and 57 per cent of total CNP fraud.

To put this into context, in 2008 when e-commerce fraud was at its peak, it cost an estimated £181.7 million. Online card fraud spending in 2008 was £41 billion. In 2012 card spending was £68 billion, up 66 per cent on 2008, while e-commerce fraud dropped 23 per cent over the same period.

Internet/e-commerce fraud losses on UK-issued cards 2002-2012
Figures in white show percentage change on previous year’s total. All figures estimated.
COUNTERFEIT CARD FRAUD

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 typically occurs as a result of criminals stealing details from the magnetic stripe on UK cards which are then used to make fake magnetic stripe cards for use overseas in countries yet to upgrade to Chip & PIN.

Counterfeit card fraud losses in the UK and abroad 2007-2012

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>2012</th>
<th>+/- change 11/12</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>12.9</td>
<td>-17%</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>29.2</td>
<td>+42%</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>42.1</td>
<td>+16%</td>
</tr>
</tbody>
</table>

Counterfeit card fraud losses on UK-issued cards 2002-2012

Figures in white show percentage change on previous year’s total

TRENDS AND STATISTICS

Counterfeit card fraud losses in the UK and abroad 2007-2012

All figures in £ millions

<table>
<thead>
<tr>
<th>Year</th>
<th>Domestic (in the UK)</th>
<th>Abroad</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>31.0</td>
<td>113.3</td>
<td>144.3</td>
</tr>
<tr>
<td>2003</td>
<td>36.2</td>
<td>133.6</td>
<td>169.8</td>
</tr>
<tr>
<td>2004</td>
<td>24.5</td>
<td>56.4</td>
<td>80.9</td>
</tr>
<tr>
<td>2005</td>
<td>16.8</td>
<td>30.8</td>
<td>47.6</td>
</tr>
<tr>
<td>2006</td>
<td>15.6</td>
<td>20.5</td>
<td>36.1</td>
</tr>
<tr>
<td>2007</td>
<td>12.9</td>
<td>29.2</td>
<td>42.1</td>
</tr>
<tr>
<td>2008</td>
<td>-17%</td>
<td>+42%</td>
<td>+16%</td>
</tr>
<tr>
<td>2009</td>
<td>-7%</td>
<td>+18%</td>
<td>+46%</td>
</tr>
<tr>
<td>2010</td>
<td>+26%</td>
<td>+18%</td>
<td>+46%</td>
</tr>
<tr>
<td>2011</td>
<td>+17%</td>
<td>+18%</td>
<td>+46%</td>
</tr>
<tr>
<td>2012</td>
<td>+25%</td>
<td>+18%</td>
<td>+46%</td>
</tr>
</tbody>
</table>

£42.1m + 16%
LOST AND STOLEN CARD FRAUD

£55.2m + 10%

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 & 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 & 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).
CARD ID THEFT

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 £7.7m | +93%
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 £24.4m | +32%
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 then arranges 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 2002-2012
Figures in white show percentage change on previous year’s total
MAIL NON-RECEIPT FRAUD

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.

Despite the increase this type of fraud remains at a very low level. It has decreased by 82 per cent in the past eight years: £72.9 million in 2004 compared with £12.8 million in 2012. At such low levels small increases are always possible and likely to seem more marked than they actually are. The increase in monetary terms over the 12 months is £1.5 million.
UK RETAILER (FACE-TO-FACE) FRAUD

Card fraud losses on the UK high street increased by 26 per cent in 2012 to £54.5 million, but are down 75 per cent since the peak losses of £218.8 million in 2004, prior to the roll out of Chip & Pin in the UK.

Undoubtedly some of the recent increase is due to the fact that fraudsters are returning to more basic crimes, finding ways of stealing both the card and the PIN in order to undertake fraudulent transactions in shops and stores. For example, criminals are targeting cards and PINs through distraction theft and shoulder surfing, as well as social engineering methods to dupe victims into handing over their cards on their own doorstep. This is because Chip & PIN has closed down opportunities for criminals in terms of compromise of cards and use in the UK.

Cards could also be used fraudulently as a result of mail-non-receipt, 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.
UK CASH MACHINE FRAUD

A portion of cash machine fraud losses are still the result of cardholders keeping their PIN written down in a 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 & PIN.

Shoulder surfing: Criminals watch the cardholder entering their PIN, then steal the card using distraction techniques or pick pocketing, before using the stolen card and genuine PIN.
FRAUD ABROAD

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 & PIN.

This increase has been driven by an increase in UK cards being compromised and used overseas in countries where Chip & PIN has not yet been rolled out (e.g. USA). However, although fraud abroad increased by 27 per cent it has to be seen in context of three years of significant decreases, driven by the banks’ fraud detection systems, which monitor for unusual spending – meaning that potential fraud is stopped before it happens. Fraud abroad losses for 2012 (£101.3m) compared with fraud abroad losses at their peak in 2008 (£230.1m), show a decrease of 56 per cent.

Fraud committed abroad on UK-issued cards 2002-2012
Figures in white show percentage change on previous year’s total
**TRENDS AND STATISTICS**

Top five countries for fraud acquired in the UK on foreign-issued cards

Losses are shown as a percentage of total fraud at UK acquired merchants on foreign issued cards.

<table>
<thead>
<tr>
<th>Year</th>
<th>Australia</th>
<th>Canada</th>
<th>France</th>
<th>Germany</th>
<th>Spain</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>38%</td>
<td>17%</td>
<td>10%</td>
<td>3%</td>
<td>3%</td>
<td>3%</td>
</tr>
<tr>
<td>2010</td>
<td>43%</td>
<td>15%</td>
<td>8%</td>
<td>5%</td>
<td>5%</td>
<td>5%</td>
</tr>
<tr>
<td>2011</td>
<td>41%</td>
<td>11%</td>
<td>9%</td>
<td>6%</td>
<td>5%</td>
<td>7%</td>
</tr>
<tr>
<td>2012</td>
<td>42%</td>
<td>9%</td>
<td>9%</td>
<td>7%</td>
<td>7%</td>
<td>4%</td>
</tr>
</tbody>
</table>

**TRENDS AND STATISTICS**

Top five countries for fraud abroad 2009-2012

UK-issued cards or card details used fraudulently overseas.

<table>
<thead>
<tr>
<th>Year</th>
<th>Australia</th>
<th>Brazil</th>
<th>Canada</th>
<th>France</th>
<th>Germany</th>
<th>Indonesia</th>
<th>Ireland</th>
<th>Italy</th>
<th>Luxembourg</th>
<th>South Africa</th>
<th>Spain</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>21.4</td>
<td>6.3</td>
<td>5.2</td>
<td>4.4</td>
<td>4.3</td>
<td>5.4</td>
<td>6.9</td>
<td>5.2</td>
<td>5.2</td>
<td>3.1</td>
<td>4.1</td>
<td>4.1</td>
</tr>
<tr>
<td>2010</td>
<td>21.5</td>
<td>5.7</td>
<td>4.8</td>
<td>3.3</td>
<td>4.3</td>
<td>4.4</td>
<td>7.9</td>
<td>5.4</td>
<td>4.4</td>
<td>3.2</td>
<td>4.4</td>
<td>4.4</td>
</tr>
<tr>
<td>2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CHEQUE FRAUD

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

COUNTERFEIT CHEQUE FRAUD £12.3m | +57%
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 £11.4m | −21%
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 £11.4m | −5%
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.
Online banking fraud refers to the fraudulent act of surreptitiously accessing and/or transferring funds from an individual’s online bank account for the purposes of financial gain. In some cases, an individual may even be duped by a criminal into making a fraudulent money transfer themselves.

A variety of factors are believed to have contributed to the increase in online banking fraud, but it has been primarily driven by a change in attack methods with criminals using phishing, social engineering scams such as vishing (phishing over the phone) in combination with more sophisticated online attacks such as infecting computers with malicious software (malware).

Online banking fraud losses are up 12 per cent in 2012 but this is only a fraction of the increase seen in phishing incidents over the last 12 months, which incidentally reduced significantly in the last quarter of 2012 (see next section).

Industry losses on online banking fraud only started to be collected from 2004 onwards.
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. Fraudsters 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. 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. Any information entered on the bogus website or form will be captured by the criminals for their own fraudulent purposes.

During 2012 the industry experienced a significant upturn in phishing volumes. The annual total number of incidents was just over 250,000, a 130 per cent increase compared to 2011. The volume of incidents reported during August (over 40,000) was the highest experienced since the start of recording in January 2005. However, during the last two months of 2012, levels of phishing activity dropped dramatically as a result of enforcement action undertaken by police.
PHONE BANKING FRAUD

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.

Industry losses on phone banking fraud only started to be collected from 2009 onwards.
INDUSTRY MEASURES

What the industry is doing to prevent payment fraud
WHAT THE INDUSTRY IS DOING TO PREVENT FRAUD

CHIP & PIN
Making card transactions safer
Chip & 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. For example:

- Counterfeit card fraud has dropped 75 per cent since it peaked in 2008.
- Fraud losses on the UK high street have fallen 75 per cent since 2004.

DEDICATED CHEQUE AND PLASTIC CRIME UNIT (DCPCU)
A specialist police unit targeting organised criminal gangs
The DCPCU is a unique pro-active police unit, with a national remit, formed as a partnership between Financial Fraud Action UK, the City of London Police and the Metropolitan Police together with the Home Office. It is fully sponsored by the cards and banking industries, with an on-going brief to investigate, target and, where appropriate, arrest and seek successful prosecution of offenders responsible for card, cheque and payment fraud crimes.

FINANCIAL FRAUD BUREAU (FFB)
The FFB is an intelligence unit 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 Strategic Threat Management Process and maintaining the industry’s Fraud Intelligence Sharing System (FISS) database. It also issues and receives intelligence alerts from the payments industry and a wide range of other stakeholders.

More information about the DCPCU can be found by visiting http://www.financialfraudaction.org.uk/Police-The-dcpcu.asp
FRAUD INTELLIGENCE SHARING SYSTEM (FISS)
Sharing intelligence to tackle fraud
FISS was established in 2008, and enables the banking industry to share information on confirmed, attempted and suspected fraud in a central, shared database. Established specifically to combat all types of banking-related fraud, the system provides the industry with a secure and robust reporting mechanism, supporting the industry’s long-term fraud prevention strategy. In 2012, the industry reported over £5.9 million of estimated savings by using FISS.

INDUSTRY HOT CARD FILE (IHCF)
Checking transactions for cards being used fraudulently
The IHCF contains information on more than 7.2 million cards reported lost, stolen or compromised. Retailers who subscribe to this electronic file come from a wide variety of business sectors, transacting on the high street, on the phone and online. 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 used successfully at French motorway tollbooths to combat the use of stolen UK cards.

TACKLING PHONE, INTERNET AND MAIL ORDER (CARD-NOT-PRESENT) FRAUD
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.
- Automated Address Verification Service (AVS) and Card Security Code (CSC) checking systems are 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.
INDUSTRY MEASURES TO PREVENT FRAUD

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 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 initiatives are in place to counter cash machine crime. These include:
- Technology upgrades to make cash machines tamper-proof, such as re-designed 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.
Industry measures 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.
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, telecommunications industry and Internet Service Providers. The industry has also worked with the National Fraud Authority and others, on joint 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 malware and phishing-related websites;
- Two-way communication with online partners to share security intelligence; and
- Information sharing between banks on counter measures against fraudulent activity.

Some banks have provided customers with two-factor authentication devices. These can be a hand-held Chip & 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.

WHAT IS THE INDUSTRY DOING TO TACKLE PHONE BANKING 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.
FFA UK works with the NFA who work with wider government, law enforcement, industry and voluntary/charity sectors to co-ordinate the fight against fraud in the UK by delivering a series of co-ordinated education and awareness campaigns, with a focus on key segments of society particularly at risk of financial fraud.

FFA UK has also been working with the NFA and other stakeholders to develop the concept of a Counter Fraud Checking Service, a way of allowing public and private sectors to bring together known frauds.

Forty organisations including The UK Cards Association and FFA UK have joined forces with the NFA to launch ‘Fighting Fraud Together’, a 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 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 organised criminal gangs 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.
FFA UK has worked closely with the City of London Police and now provides a regular fraud intelligence feed from its Fraud Intelligence Sharing System (FISS).

PCeU
The Police Central e-Crime Unit (PCeU) is helping to tackle e-crime fraud losses by leading investigations, providing specialist police officer training and co-ordinating cross-force initiatives to crack down on online criminals.
FFA UK works closely with the Unit, for example by providing witness statements, MI analysis and data repatriation.

BRITISH BANKERS ASSOCIATION (BBA)
FFA UK works closely with the BBA on financial crime matters of mutual interest, including co-branding advice to consumers on issues such as money mules and investment fraud.

NATIONAL CRIME AGENCY (NCA)
FFA UK has been involved in advising on the set-up and structure for the Economic Crime Command under the NCA, and in particular is working with the NCA on its Economic Crime Command Intelligence Hub, which links with the proposed Counter Fraud Checking Service under the NFA.
COMMON SCAMS & ADVICE

How to minimise the chances of becoming a victim of fraud
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.
CARD FRAUD TELEPHONE CRIME (‘COURIER FRAUD’)

This scam involves a person being called by a criminal posing as someone from their bank, or even the police. The caller tells the victim that their credit or debit card needs collecting and replacing following fraud on their account. Police have found that the criminal caller reassures the victim that the call is genuine by getting them to hang up and call the bank’s number for confirmation. Following this, the criminal caller stays on the line, tricking the victim into believing they are on a new call and that the person at the end of the line is their bank.

The criminal caller will then either ask the person for their PIN or ask them to key their PIN number into their telephone keypad, before sending a courier to collect the card. The victim is told that the card is going to the bank, but actually is delivered to the fraudster along with the PIN obtained during the scam.

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 and come with a criminal sentence of up to 10 years. Money mules are the easiest part of the chain to track down.
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 bankers’ draft is advised not to hand over the goods until they have certainty that the 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 bankers’ 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]. To confirm when the proceeds of a cheque will be yours, use the cheque checker provided at www.chequeandcredit.co.uk

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 obvious signs of 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.

FRAUD PREVENTION ADVICE

AVOIDING CARD 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.
- 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 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 or bankers’ draft 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 counterfeit.

- If sending a cheque in the post, make sure that it cannot be identified as a cheque through the envelope (enclose the cheque in a folded sheet of paper, for example).

- 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 transactions will be below your bank’s Faster Payment limit, 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 bankers’ 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.
PREVENTING FRAUD ONLINE AND OVER THE PHONE

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 terms, 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.

General advice

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.
- 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.
ADVICE WHEN USING A DIGITAL WALLET

- If you access your digital wallet using a password, do not share the password with anyone and select a password that cannot be easily guessed.
- Make sure you change your digital wallet password regularly or immediately if you suspect that someone might know it.
- When accessing your digital wallet via your smart device or at your PC (for example, to check your account balance or to add the details of an additional card), if not using an App, always type the URL into the browser. Never enter the wallet via e-mail links.
- When making a purchase using your digital wallet at a retailer that is unfamiliar to you, try to find out more about them before undertaking the transaction. Do you know their contact phone number (not just a mobile phone number) and their physical postal address (not just a post office PO Box number)?

ADVICE WHEN USING A MOBILE BANKING APP

- Only use official bank Apps (and websites) to do your banking. Check the App has been published by your bank.
- Only download mobile Apps from official stores, such as Apple iTunes, Android Marketplace and Blackberry App World. Free Apps are great but downloading them from unknown sources could lead to your device becoming infected with a virus.
- Users should look carefully at reviews of the developer/company who publish the App.
- Review and understand the permissions you are giving when you download Apps.
- Advise your bank immediately if you feel someone may know your log in details for your mobile banking App or if you lose your smart device. Your bank can then stop the service to your device.
- Smart devices require updates to run Apps and firmware. If the device users neglect this, it increases the risk of the device being hacked or compromised.
- When using a mobile App always log out when you have finished using it.
- Be aware of and ignore phishing emails that may request personal details and credentials used to log in to your banking App.
ADVICE WHEN USING A MOBILE PHONE CARD READER

Chip & PIN card readers that use Bluetooth via an app on your smart device (e.g., mobile phones or tablet) or card readers that plug into a mobile phone or tablet are increasingly being used by small traders such as plumbers and window cleaners to accept a card payment from their customers (similar to the types of card payments made in a shop or store). When paying this way your card is usually swiped or inserted into a reader attached to the small trader’s device and you are then either prompted to sign or enter your four digit PIN.

- Make sure you are dealing with a small trader that you trust before making a transaction.
- If prompted to enter your PIN, ensure that you shield the keypad, so that your PIN cannot be seen by anyone else. If you suspect someone knows your PIN, change it immediately at a cash machine.
- Keep your card within your sight at all times.
- Ensure you receive a receipt for your transaction – this may be provided via e-mail.
- Regularly check your statements and report any suspicious transactions to your bank.

ADVICE WHEN USING MOBILE TO MOBILE PAYMENTS

Mobile to mobile payments allow bank account customers to send and receive payments through their smart device offering an easy way to pay a friend back for dinner. You are normally required to download an App to your smart device as well as register/be registered in order to use the service and simply need to know the payment recipient’s mobile telephone number (rather than their bank account details).

- Keep your smart device secure i.e. use of a PIN.
- Do not divulge your login details to anyone.
- Ensure the application is the official version.
- Avoid sharing with anyone the phone you bank on.
- Be sure to clear your browsing history, cache and cookies on a regular basis.
- Make sure that your phone operating system is up to date.
- When you have finished using the App, ensure you log out properly.
ADVICE WHEN USING CONTACTLESS CARD PAYMENTS

- Contactless cards benefit from the same range of advanced security features found on a standard Chip & PIN card; and transactions are processed through the same secure networks.
- Although Contactless transactions don’t require a PIN, sometimes you will be prompted to insert your card into the Chip & PIN reader and enter your PIN. This security check is in place to protect you from fraud and your card company restricts how much your card can be used before you will need to provide a PIN.
- Along with these precautions, the £20 limit on Contactless transactions reduces the potential for fraud. For transactions over £20 you will need to use Chip & PIN in the usual way.
- It’s worth remembering that if your wallet is stolen you won’t normally get your cash back, but if you are the innocent victim or debit or credit card fraud you will not be liable for any fraud losses. This is regardless of whether or not your cards carry the Contactless functionality.
- Always take reasonable steps to keep your PIN and any security information secure, and if your card is lost or stolen report it to your card company as quickly as possible.

ADVICE WHEN USING MOBILE CONTACTLESS PAYMENTS

As with use of a contactless card in shops and stores the customer simply holds their smart device (e.g. mobile phone or tablet) against a secure reader when instructed to do so by the shop staff:

- Mobile contactless payments enjoy exactly the same protection as standard contactless cards with the added benefit that you are able to turn off the application when you do not want to use it.
- Ensure that your mobile contactless payment application is protected with a PIN (we would not recommend you use your bank card PIN). You may be given the option to set up the applications to require you enter the PIN for all transactions or, where higher value payments are supported, only for transactions that exceeds the £20 limit.
- If you lose your phone, report the loss to your card issuer who will be able to block the mobile contactless payment application and ensure that service is restored to any new device you are given.
FURTHER ADVICE REGARDING SMART DEVICES (MOBILE PHONES OR TABLETS)

- Never give your mobile banking security details, including your login details, to anyone else and do not store these on your smart device (e.g. mobile phone or tablet).
- Do not store account details, passwords, bank account numbers, PINs or credit or debit card details on your mobile phone.
- For added security password or PIN protect your smart device. This is the first layer of physical security to protect the contents of the device. In addition to a PIN, enable the screen lock feature so that your device automatically locks after a few minutes of inactivity. It can then be re-opened using your PIN.
- Never leave your smart device unattended when logged on, watch out for people looking over your shoulder, and consider using privacy screens with any tablet device.
- Think carefully before removing any security controls from your smart device, this is known as jail-breaking or rooting your device. This may weaken the security of your device and expose you to additional risks.

- If possible, keep your smart device’s operating system updated with the latest security patches and upgrades. Older software may have security vulnerabilities that could expose you to additional risks. Also consider using a reputable brand of anti-virus software on your smart device. Some banks offer customers free anti-virus software for their mobile phones; check your bank’s website.
- Avoid clicking on or otherwise downloading software or links from unknown sources.
- Be cautious about opening links contained in SMS messages or emails. Don’t respond to unsolicited messages and remember that your bank will never contact you to ask you to disclose your security credentials.
- Do not allow your smart device to connect to unknown wireless networks. These networks could be rogue access points that capture information passed between your device and your legitimate server.
- Use the same precautions on your smart device as you would on your computer when using the internet.
- If you decide to sell your smart device or trade it in, make sure you wipe it first (reset it to factory default) to avoid leaving personal data on the device.
Make a note of your smart device’s International Mobile Equipment Identity (IMEI) number. This is a unique 15 digit number that identifies your device to your provider. If your device is ever lost or stolen, your mobile provider can use this number to block and permanently deactivate the device, therefore making it useless to anyone who has the device. The IMEI number is usually found printed in the battery compartment or you can access it on most devices by entering the key sequence *#06#.

Register your smart device with Immobilise (www.immobilise.com). This registration enables the police to return the device back to you if it is ever recovered.

Ensure that your Bluetooth is switched off when you do not need to use it.

Be aware of the practice of ‘Smishing’ – where criminals send unsolicited text messages to a mobile phone number, with the intention of inducing the recipient to believe that it is from their bank, instructing that someone is trying to send money and asking the mobile phone user to visit the fraudster’s fake website and provide their personal details.

A Quick Response (QR) code is a type of matrix barcode that can store alphanumeric characters, in the form of texts or URLs. All you need to visualise such a code is a smart device with a camera and a QR reader application to scan it. The code can direct you to websites or online videos, send text messages and e-mails, or launch Apps. Fast, easy and very popular, scanning QR codes are clearly a convenient way to stay informed anytime, anywhere. But the downside is that you don’t really know the content of a QR code until you scan it. For this reason you must be careful when scanning one, as your device’s security might be at risk. Criminals might use these codes to redirect you to websites via malicious links that then ask you to download malicious applications containing a virus or malware.
FREQUENTLY ASKED QUESTIONS

What should I do if I think I am 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.

Will I be held liable for fraud on my credit or debit cards, phone/online banking or cheques?
If you are an innocent victim of fraud you have legal protection which means that you will not be liable for any losses unless you have acted fraudulently or without reasonable care.

What should I do if I have a complaint about my bank or card issuer?
If you have a complaint about your card issuer your first step should be to contact them directly. If you are unable to resolve the issue by going through their complaints procedure then you can contact the Financial Ombudsman. For further information please visit www.financial-ombudsman.org.uk

What should I do if I have a complaint about a retailer with regard to a purchase I have made?
In the first instance, you should contact the retailer with full details of the problem. If the issue is not resolved to your satisfaction, you should contact your bank or card company and inform them of the disputed transaction. After you have contacted your bank or card company you can contact Trading Standards who provide consumer protection information in the UK. For further information visit www.tradingstandards.gov.uk

What should I do if my cards are stolen?
If your cards have been stolen, contact your card issuer and the police immediately.

I need to report my card lost/stolen. Where can I find the emergency contact number for my bank/card company?
Emergency Contact details can be found here: http://www.financialfraudaction.org.uk/Consumer-Emergency-Contact-Details.asp
What is identity theft?
This occurs when sufficient information about an identity is obtained to facilitate identity fraud, irrespective of whether, in the case of an individual, the victim is alive or dead. Identity theft can result in fraud affecting consumers’ personal financial circumstances as well as costing the government and financial services millions of pounds a year.

Identity theft is also known as impersonation fraud. It is the misappropriation of the identity (e.g. name, date of birth, current or previous addresses) of another person without their knowledge or consent.

I have given out my personal details, and now I am concerned about identity theft. What should I do?
If you have given out your card details and are concerned as to how they will be used you should contact your card issuer immediately. Your card issuer will be able to advise you of the best action to take in your particular circumstances.

In the case that you are issued with new card details, fraudsters should not be able to undertake any fraudulent card-not-present (internet shopping, telephone or mail order) activity on your account.

By just giving out your card details you are not automatically going to become a victim of identity theft.
You may consider contacting CIFAS – the UK’s Fraud Prevention Service to apply for protective registration if you believe you are a victim of identity fraud or at risk of becoming one. Once you have registered, CIFAS members will carry out extra checks whenever anyone, including you, applies for a financial service using your address. They do this to make sure that a criminal is not trying to commit fraud by pretending to be you. You will have to pay a charge for this service.

Check your personal credit file and statements from your bank and credit card company for any suspicious entries or transactions. Your credit file can be obtained from a credit reference agency.

Credit Reference Agencies to contact are:
- Experian
- Equifax
- CallCredit
Why did the industry introduce Chip & PIN if contactless technology relies on neither a PIN nor a signature; how are customers authenticated?

Contactless cards have been introduced because of the convenience they offer. The introduction of Chip & PIN in the UK means contactless technology has been rolled out in a secure environment. The precautions in the system draw a sensible balance between maintaining convenience and limiting the risk of financial loss – contactless transactions are limited to a maximum of £20.

From time to time, when undertaking contactless transactions, you will be asked to perform a full Chip & PIN transaction. When you enter your PIN – either in this situation at an ATM, or when performing a Chip & PIN transaction for high value purchases – this confirms you are still in possession of your card.

I have heard that contactless cards can be copied at a distance by fraudsters using fake card readers. Is this true?

The contactless application does not increase the risk of contactless cards being cloned. The data stored on the contactless application is limited, and is not the same as that stored on the magnetic stripe. Any contactless data that could be read cannot be used to make a cloned card that would work.

A contactless card reader can interrogate your card provided it is within ten centimetres of the card. However a contactless card will only release a limited set of data (the same details that can also be seen on the front of the card) which a fraudster would find very difficult to use elsewhere, and couldn’t be used to make a cloned card that would work.
What should I do if I have been sent a phishing email?
Any unsolicited emails should always be approached with caution, and you are advised not to follow any links contained in the email or to give out any personal details.
This is a very common fraud, and you should ignore all such emails. Do not correspond with the sender.
For more information about phishing go to www.banksafeonline.org.uk

I’ve been offered a job as a money transfer agent. I am suspicious that this is not a genuine job offer. Should I accept?
Money mules are commonly recruited via job advertisements for ‘payment processing agents’, ‘money transfer agents’ or ‘local processors’. Other recruitment methods include spam e-mails, instant messaging and adverts in newspapers. Candidates are asked to accept payments and to remit most of the funds to a third party – a job which can be done from one’s own home. Legitimate companies use escrow services for this kind of work.
Allowing your bank account to be used for fraud is illegal and can result in ten years in prison.
CONTACTS
Details of organisations helping in the fight against fraud
USEFUL CONTACTS

www.actionfraud.org.uk
Action Fraud is the UK’s national fraud reporting centre where you should report fraud if you have been scammed or defrauded.

www.bacs.co.uk
Bacs Payment Schemes Limited (originally Bankers’ Automated Clearing Services) is a United Kingdom scheme for the electronic processing of financial transactions.

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

www.bba.org.uk
The BBA is the leading trade association for the UK banking and financial services sector.

www.bsa.org.uk
The Building Societies Association is a trade association, representing mutual lenders and deposit takers in the UK.

www.chapsco.co.uk
CHAPS is the only UK payment system that guarantees real-time finality, of any value, in “Central Bank money” as each payment instruction settles.

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.

www.cifas.org.uk
CIFAS is a not-for-profit membership association representing the private and public sectors.

www.crimestoppers-uk.org
Crimestoppers is an independent charity working to fight crime.

www.fasterpayments.org.uk
Faster Payments Service (FPS) is a UK banking initiative to reduce payment times between different banks’ customer accounts.

www.fca.gov.uk
The Financial Conduct Authority is a quasi-governmental agency in the UK, formed as one of the successors to the Financial Services Authority.

www.financialfraudaction.org.uk
Financial Fraud Action UK is the name under which the financial services industry co-ordinates its activity on fraud prevention, representing a united front against financial fraud and its effects.
www.financial-ombudsman.org.uk
Provides assistance in resolving complaints against bank, building society, financial adviser, insurance company, investment firm, stockbroker or unit trust company.

www.getsafeonline.org
Sponsored by government and leading businesses to help protect individuals against Internet threats.

www.lendingstandardsboard.org.uk
Ensures that banks and building societies comply with the lending codes, and also interprets and develops the codes.

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

www.gov.uk/government/organisations/national-fraud-authority/about
The National Fraud Authority (NFA) works with wider government, law enforcement, industry and voluntary/charity sectors to coordinate the fight against fraud in the UK.

www.paymentscouncil.org.uk
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.

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

www.tradingstandards.gov.uk
The Trading Standards Institute is a professional membership association formed in 1881. It represents trading standards professionals in the UK and overseas – in local authorities, the business and consumer sectors and in central government.

www.tuff.co.uk
A forum for the exchange of information and the promotion of a united effort against telecommunications fraud.

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

This document is provided for information purposes only. While every effort is made to ensure the accuracy of any information or other material contained in this document, it is provided on the basis that UK Payments Administration Ltd (and members of its various committees, either individually or collectively) accept no responsibility for any loss, damage, cost or expense of whatsoever kind arising directly or indirectly from, or in connection with, the use by any person of any information or other material contained therein. Any use of the information or other material contained in this document shall signify agreement to this provision.

© UK Payments Administration Ltd 2013. Published by the UK Payments Administration Ltd.