The definitive overview of payment industry fraud and measures to prevent it
Financial Fraud Action UK (FFA UK) is responsible for leading the collective fight against fraud in the UK payments industry. Our membership includes banks, credit, debit and charge card issuers, and card payment acquirers in the UK. We provide a forum for our members to work together on non-competitive issues relating to financial fraud. Our primary function is to facilitate collaborative activity between industry participants and with other partners.

Our key aims are to:

- Provide a single cohesive industry voice on financial fraud
- Lead collaborative industry-wide activity to prevent and control financial fraud
- Uphold the reputation of the industry by demonstrating its record on fraud prevention

We do this by:

- Sponsoring the Dedicated Card and Payment Crime Unit, a unique pro-active operational police unit, with a national remit, formed as a partnership between FFA UK, the City of London Police, and the Metropolitan Police
- Managing the Industry Strategic Threat Management Process, which provides an up-to-the-minute picture of the threat landscape
- Delivering UK-wide awareness campaigns to inform customers about threats and how to stay safe
- Managing intelligence-sharing through the industry fraud intelligence hub (Financial Fraud Bureau) and the Fraud Intelligence Sharing System (FISS) which feeds intelligence to police and other agencies in support of law enforcement activity
- Informing commentators and policy-makers through a press office and public affairs function
- Providing expert security assessments of new technology, as well as the impact of new legislation and regulation
- Publishing the official fraud losses for the UK payments industry, as well as acting as the definitive source of industry fraud statistics and data

The industry continues to face the challenge of criminals using scams and computer attacks to trick people into disclosing their personal details or parting with their money. Raising public awareness is key to beating the fraudsters. Last year we launched a major campaign, centred on a Joint Declaration of all UK banks and supported by national advertising, helping people to spot the signs of a scam. At the same time the industry is persistently enhancing fraud detection measures to protect consumers, and tackling the organised criminal gangs behind payment fraud by funding a specialist police unit – the Dedicated Card and Payment Crime Unit.

KATY WOROBEC, Director FFA UK
CONTENTS

Trends and statistics 7
Card fraud 8
- Fraud losses on UK-issued cards 2004–14 8
- Annual fraud losses on UK-issued cards 2004–14 8
- Annual case volumes on UK-issued cards 2008–14 9
- Fraud to turnover ratio 2004–14 10
- Card fraud losses split by type 11
- Remote purchase fraud 12
- Counterfeit card fraud 13
- Lost and stolen card fraud 14
- Card ID theft 15
- Card non-receipt fraud 16
- Card fraud losses on the UK high street 17
- Internet/e-commerce fraud 18
- Card fraud at UK cash machines 19
- Card fraud abroad 20
Cheque fraud 22
Online banking fraud 23
Phone banking fraud 24
Phishing 25

Industry measures 27
Common scams and advice 35
Common scams 36
Fraud prevention advice 40
Frequently asked questions 52

Contacts 57
TRENDS AND STATISTICS

An overview of the different types of fraud and a summary of fraud trends
CARD FRAUD

Fraud losses on UK issued cards totalled £479.0 million in 2014, a 6% increase from £450.4 million in 2013; the third consecutive year of increase. For the first time FFA UK is also publishing the number of fraud incidents to convey more fully the dynamics of the fraud environment in the UK. The data follows much the same trend as fraud by value, with 2014 figures down on the peak of 2008. However losses are still 21% lower than the peak of £609.9 million seen in 2008. In fact, the number of genuine card transactions has increased from 10.5 billion in 2008 to 15.8 billion in 2014 – a 51 per cent rise with the total value spent rising from £602 billion to £802 billion – a 33 per cent rise, yet in the same time period overall card fraud losses have decreased 21 per cent.

Overall card fraud losses as a proportion of the amount we spend on our cards has increased only slightly during 2014, rising from 7.4p per £100 spent in 2013 to 7.5p in 2014. (In 2008 it was 12.4p for every £100 spent).

These trends owe much to the use of deception crimes, as well as the use of online attacks, such as malware and data hacks, to compromise card details. In response, the industry has redoubled its efforts to warn consumers and online businesses to install security software which is often available free from a customer’s own bank. To prevent stolen card details being used to make purchases online, retailers are advised to take steps to improve their security, including use of online protection services (including American Express ‘SafeKey’, ‘Verified by Visa’ and MasterCard ‘SecureCode’).
Annual case volumes on UK-issued cards 2008 to 2014

It is important to note that number of cases relates to the number of accounts that have been defrauded, as opposed to the number of victims.

<table>
<thead>
<tr>
<th>Card fraud type</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>% change 13–14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote purchase fraud</td>
<td>875,086</td>
<td>824,736</td>
<td>733,145</td>
<td>709,402</td>
<td>750,200</td>
<td>951,998</td>
<td>1,019,146</td>
<td>+7%</td>
</tr>
<tr>
<td>Counterfeit (skimmed/cloned) fraud</td>
<td>371,442</td>
<td>177,430</td>
<td>96,861</td>
<td>81,112</td>
<td>98,322</td>
<td>101,109</td>
<td>99,279</td>
<td>-2%</td>
</tr>
<tr>
<td>Fraud on lost or stolen cards</td>
<td>115,590</td>
<td>99,403</td>
<td>101,947</td>
<td>104,467</td>
<td>113,003</td>
<td>138,967</td>
<td>133,943</td>
<td>-4%</td>
</tr>
<tr>
<td>Card ID theft</td>
<td>26,488</td>
<td>20,736</td>
<td>19,555</td>
<td>15,420</td>
<td>24,078</td>
<td>30,718</td>
<td>26,542</td>
<td>-14%</td>
</tr>
<tr>
<td>Card non-receipt</td>
<td>10,839</td>
<td>8,302</td>
<td>6,622</td>
<td>8,536</td>
<td>9,018</td>
<td>9,125</td>
<td>9,302</td>
<td>+2%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>1,399,445</td>
<td>1,113,607</td>
<td>958,130</td>
<td>918,937</td>
<td>994,621</td>
<td>1,231,917</td>
<td>1,288,212</td>
<td>+5%</td>
</tr>
</tbody>
</table>

Fraud to turnover ratio 2004–2014

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

Card fraud losses split by type (as percentage of total losses)
REMOTE PURCHASE FRAUD (INTERNET, TELEPHONE, MAIL ORDER)

The vast majority of this type of fraud involves the use of card details that have been fraudulently obtained through methods such as skimming, digital attacks such as malware and data hacks, 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. It is also known as ‘card-not-present’ (CNP) fraud.

Online fraud against UK retailers totalled an estimated £136.6 million in 2014, a rise of 10% on the previous year. However, there was a substantial rise in fraud against online retailers based abroad, rising 22% to £80.8 million.

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.
LOST AND STOLEN CARD FRAUD

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 £10.2m (+16%)

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 £19.7m (-29%) 

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.
CARD NON-RECEIPT FRAUD

This type of fraud involves cards being stolen whilst in transit – after the card company sends them out and before the genuine cardholder receives 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.

PLEASE NOTE: Figures in the following sections relate to the places where the card was used fraudulently rather than how the card or card details were compromised. This is simply another way of breaking down the overall plastic card fraud totals and so these figures should not be treated as an addition to those already covered in the earlier sections. Case volumes are not available for the place of misuse as it is feasible that one case could cover multiple places of misuse. E.g. a lost or stolen card could be used to make an ATM withdrawal and also purchase goods on the high street.

CARD FRAUD LOSSES ON THE UK HIGH STREET

Fraud losses on face to face purchases on the UK high street decreased by 14% in 2014 to £49.2 million. Losses are 78% lower than the peak of £218.8 million in 2004, prior to the roll out of Chip & PIN in the UK.

The majority of this fraud is undertaken using more basic techniques, with fraudsters finding ways of stealing both the card and PIN in order to carry out 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 to compromise cards and use them on the high street.

Card non-receipt fraud losses on UK-issued cards 2004–2014


Figures in white show percentage change on previous year’s total
INTERNET/E-COMMERCE FRAUD

These figures are included within the overall remote purchase (CNP) fraud losses described in the previous section. An estimated £217.4 million of e-commerce fraud took place on cards in 2014, accounting for 45% of all card fraud and 66% of total remote purchase fraud.

E-commerce fraud has now reached its highest point since data collection began in this area. However, this is to be expected given the considerable increase in genuine usage in this channel over the last 10 years with spending reaching £175 billion in 2014, meaning that for every £100 spent on the internet only 12.4p is fraudulent.

NB: These figures include spending and losses outside the UK.

CARD FRAUD AT UK CASH MACHINES

These figures show how much fraud takes place at cash machines in the UK on stolen cards or where a card account has been taken over by the fraudster: in all cases the fraudster would need to have access to the genuine PIN and card. Some losses result from 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 in three main ways:

- **Entrapment devices:** Inserted into a cash machine’s card slot, these devices retain the card inside the 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 subsequently withdraws cash.

- **Skimming devices:** Attached to the cash machine to record the details from the magnetic stripe of a card whilst a miniature camera captures the PIN being entered. A fake magnetic stripe card is then produced and used with the genuine PIN to withdraw cash at 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.

FRAUD LOSSES AT UK CASH MACHINES 2004–2014

<table>
<thead>
<tr>
<th>Year</th>
<th>£ millions</th>
<th>% change</th>
<th>£ millions</th>
<th>% change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>74.6</td>
<td>-12%</td>
<td>65.8</td>
<td>-4%</td>
</tr>
<tr>
<td>2006</td>
<td>62.0</td>
<td>-6%</td>
<td>62.0</td>
<td>-4%</td>
</tr>
<tr>
<td>2007</td>
<td>45.7</td>
<td>+31%</td>
<td>35.0</td>
<td>+6%</td>
</tr>
<tr>
<td>2008</td>
<td>36.7</td>
<td>-9%</td>
<td>33.2</td>
<td>-7%</td>
</tr>
<tr>
<td>2009</td>
<td>29.3</td>
<td>+10%</td>
<td>28.9</td>
<td>+10%</td>
</tr>
<tr>
<td>2010</td>
<td>23.1</td>
<td>-15%</td>
<td>23.1</td>
<td>-15%</td>
</tr>
</tbody>
</table>

Figures in white show percentage change on previous year’s total. All figures estimated. *We have made an improvement to the way in which we estimate e-commerce fraud. This has only been applied to 2013 and 2014 figures hence the apparent large increase in 2013.*
The majority key driver for this type of fraud is where criminals steal magnetic stripe details from UK cards to make counterfeit cards for use overseas in countries yet to upgrade to Chip & PIN. Remote purchase fraud at overseas retailers is also included in these figures.

International fraud losses for 2014 were £150.3 million compared with losses at their peak in 2008 (£230.1m), a decrease of 35%.

Fraud committed abroad on UK-issued cards 2004–2014

Top five countries for fraud abroad
UK-issued cards or card details used fraudulently

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
**CHEQUE FRAUD**

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

**Counterfeit cheque fraud £5.5m (-24%)**

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 £6.7m (-41%)**

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 £5.6m (-37%)**

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**

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 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).

Industry losses on online banking fraud were only collected from 2004 onwards.
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, vishing (often pretending to be from a bank or the police) and bin-raiding.

Industry losses on phone banking fraud were only collected from 2009 onwards.

Phone banking fraud losses 2004–2014

<table>
<thead>
<tr>
<th>Year</th>
<th>Value (£ millions)</th>
<th>% change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>NA</td>
<td>0%</td>
</tr>
<tr>
<td>2005</td>
<td>NA</td>
<td>0%</td>
</tr>
<tr>
<td>2006</td>
<td>NA</td>
<td>0%</td>
</tr>
<tr>
<td>2007</td>
<td>NA</td>
<td>0%</td>
</tr>
<tr>
<td>2008</td>
<td>12.1</td>
<td>+5%</td>
</tr>
<tr>
<td>2009</td>
<td>12.7</td>
<td>+32%</td>
</tr>
<tr>
<td>2010</td>
<td>16.7</td>
<td>+22%</td>
</tr>
<tr>
<td>2011</td>
<td>12.6</td>
<td>-25%</td>
</tr>
<tr>
<td>2012</td>
<td>11.6</td>
<td>-8%</td>
</tr>
<tr>
<td>2013</td>
<td>13.9</td>
<td>+20%</td>
</tr>
<tr>
<td>2014</td>
<td>13.9</td>
<td>+20%</td>
</tr>
</tbody>
</table>

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

Phishing describes the practice of sending emails at random, purporting to come from a genuine company such as a bank, but increasingly other organisations such as HMRC, 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.

Number of phishing websites targeted against UK banks and building societies 2005–2014

<table>
<thead>
<tr>
<th>Year</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>1,700</td>
</tr>
<tr>
<td>2006</td>
<td>14,156</td>
</tr>
<tr>
<td>2007</td>
<td>25,797</td>
</tr>
<tr>
<td>2008</td>
<td>43,991</td>
</tr>
<tr>
<td>2009</td>
<td>51,161</td>
</tr>
<tr>
<td>2010</td>
<td>61,873</td>
</tr>
<tr>
<td>2011</td>
<td>111,286</td>
</tr>
<tr>
<td>2012</td>
<td>256,641</td>
</tr>
<tr>
<td>2013</td>
<td>26,995</td>
</tr>
<tr>
<td>2014</td>
<td>23,729</td>
</tr>
</tbody>
</table>

Please note: case volumes were not collected in this area until 2012
INDUSTRY MEASURES

What the industry is doing to prevent payment fraud
DEDICATED CARD AND PAYMENT CRIME UNIT (DCPCU)

The Dedicated Card and Payment Crime Unit (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. It is headed up by a Detective Chief Inspector and comprises officers from the Metropolitan and City of London police forces who work alongside banking industry fraud investigators and support staff. Since its inception in 2002, the unit has:

- Achieved £470 million in savings from reduced fraud – with the current level of savings equivalent to over £800,000 per week
- Recovered 75,000 counterfeit cards
- Recovered 596,000 compromised card numbers
- Secured 315 convictions on fraud related matters
- Upheld a conviction rate of 94%

More information about the DCPCU can be found by visiting www.financialfraudaction.org.uk/Police-The-dcpcu.asp

FINANCIAL FRAUD BUREAU (FFB)

Established in 2010, the Financial Fraud Bureau (FFB) leads the payments industry’s collective initiatives on fraud data-sharing. Its key roles are:

- Disseminating intelligence directly from, and to, police forces and other law enforcement organisations
- Gathering, collating and analysing the intelligence that informs the Industry Strategic Threat Management Process
- Managing the Fraud Intelligence Sharing System (FISS) database
- Issuing and receiving intelligence alerts from the payments industry and a range of other stakeholders.

Through the FFB, the industry can be alerted immediately of any known compromise of bank or card data through a series of designated Single Point of Contact (SPOCs). A memorable example was the loss of data in 2007 by the HMRC of 8.2 million bank accounts used by child benefit recipients. The FFB ensured that details of these accounts were quickly and securely alerted to all the affected banks so that customers could be protected. In another illustration, the industry co-ordinated law enforcement and supermarket security representatives – alongside banks and card schemes – to tackle a series of organised gangs, the members of which were tampering with PIN entry devices in order to obtain card details.

FRAUD INTELLIGENCE SHARING SYSTEM (FISS)

Sharing data and intelligence to tackle fraud

The Fraud Intelligence Sharing System (FISS) is a central industry database – an extremely secure, flexible and cost-effective intelligence system designed to support the card and retail banking industries in the fight against fraud. It can be used to identify linkages and patterns in frauds thereby playing an important role in protecting consumers.

Members exchange a range of information on fraud, which offers the benefit of sector-wide intelligence sharing in a flexible format. This helps industry and police to identify patterns and strengthen defences. Importantly, the FISS allows the supply of fraud data and intelligence collated by the payments industry to the National Fraud Intelligence Bureau.
TACKLING REMOTE PURCHASE (CNP) 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 pre-register their card or register when prompted, and create a password. These services assess each transaction and either verify it automatically or, in some cases, ask cardholders to provide the password to help verify the payment.

**Address Verification Service (AVS)** and **Card Security Code (CSC)** checking systems are available for UK businesses that accept phone, internet or mail order transactions. These services allow merchants to verify the delivery address to the card billing address of a cardholder and to cross-check the security code on the signature strip of the card to prove the card number is genuine. These data checks provide additional information to help businesses assess fraud risks and decide whether to proceed with the transaction.

**Cyber Streetwise** FFA UK partnered with the Home Office to deliver a remote payment fraud awareness online animated video as part of the Government’s wider Cyber Streetwise campaign. The video is aimed at small businesses that accept card payments online, and has overarching messages regarding the importance of ‘Knowing Your Customer’ and online authentication, encouraging small merchants to utilise MasterCard SecureCode, Verified by Visa and American Express SafeKey. The video has had over 1 million views and can be found at: [www.youtube.com/watch?v=XYNOZmhF6b8&feature=youtube](http://www.youtube.com/watch?v=XYNOZmhF6b8&feature=youtube)

**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 72% since it peaked in 2008
- Fraud losses on the UK high street have fallen 78% since 2004

**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 63% 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.

Initiatives are continuously being rolled out 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 or a PIN recording camera.
- 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, shielding your PIN and 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

INDUSTRY HOT CARD FILE (IHCF)
Checking transactions for cards being used fraudulently
The IHCF contains information on cards reported lost, stolen or compromised. 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. Retailers who subscribe to this electronic file come from a wide variety of business sectors, including online shopping businesses who have a time delay between taking an order and its despatch, and therefore make use of the IHCF as a mechanism to provide continued checks on the validity of the card used for payment during this period. This allows them the opportunity, before goods are dispatched, to verify the order with the purported cardholder and to terminate delivery if fraud is discovered. The IHCF is also used successfully at French motorway tollbooths to combat the use of stolen UK cards.

CHEQUE FRAUD
Industry measures to protect customers
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 after the end of the sixth working day after paying in a cheque or bankers’ draft 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.

Industry measures to prevent cheque fraud
Both the banks and the wider industry employ a number of measures to prevent cheque fraud. The identification of lost, stolen or fraudulent cheques, as they are processed through the clearing system, has reduced the instances of fraud being realised. In the past year the banking industry successfully identified over 90% of all fraudulent cheques as they went through the cheque clearing process.

The Cheque Printer Accreditation Scheme (CPAS), set up in 1995 and managed by the Cheque and Credit Clearing Company, has been used to combat cheque fraud. 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. All cheques that are meant for use in Great Britain must be printed by a CPAS member.

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 National Crime Agency, the Metropolitan Police Cyber Crime Unit (MPCCU), overseas law enforcement agencies, technology companies, anti-virus firms, telecommunications industry and Internet Service Providers. The industry has also worked with government and others, on joint campaigns to raise awareness of various types of online fraud and provide helpful security advice to consumers and businesses.

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.

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.financialfraudaction.org.uk to help online and telephone banking users stay safe online.
COMMON SCAMS AND ADVICE
How to minimise the chances of becoming a victim of fraud
VISHING

‘Vishing’ involves a fraudster phoning a potential victim and posing as someone from a bank or building society, the police or another legitimate organisation such as a telephone or internet provider.

They attempt to obtain financial information which often includes credit or debit card details (including PIN), bank account details and personal information such as full name, date of birth or address.

This information is used by the fraudster to gain access to their victim’s finances. The fraudster sometimes even deceives the victim to transfer money themselves from their bank account to one which is accessible to the fraudster.

A variation on this scam involves the victim being persuaded to withdraw money from a branch or cash machine to pay to the fraudster.

Your bank or the police will never:

- Phone you to ask for your 4-digit card PIN or your online banking password, even by tapping them into the telephone keypad.
- Ask you to withdraw money to hand over to them for safe-keeping.
- Ask you to transfer money to a new account for fraud reasons, even if they say it is in your name.
- Send someone to your home to collect your cash, PIN, payment card or cheque book if you are a victim of fraud.
- Ask you to purchase goods using your card and then hand them over for safe-keeping.

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.

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 ten 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. 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.

To see all education and awareness campaigns, please see www.financialfraudaction.org.uk/consumer-advice.asp

KEEP IT SECRET, KEEP IT SAFE – PROTECT YOUR PIN

1. NEVER share your PIN with anyone – the only times you should use your PIN are at a cash machine or in a shop.
2. 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.
3. Your bank will NEVER ask you to authorise anything by entering your PIN into the telephone.
4. 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.
5. 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 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**

- Don’t accept a cheque, or banker’s draft from someone, unless you know and trust them.
- Consider asking for or using alternative payment methods, such as CHAPS or Faster Payments, for high value items, such as selling your 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.
- Don’t release goods for sale until you have confirmed that the proceeds of a cheque of bankers draft have cleared. To find out when you can be sure that the proceeds of a cheque are yours to keep, use the cheque checker at www.chequeandcredit.co.uk
- 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).
- 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.

For more information go to www.chequeandcredit.co.uk/resources/faqs/cheque_fraud/-/page/2322/

PREVENTING FRAUD ONLINE

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 pre-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.

Banking online
As additional preventative measures when banking online, you should:
- 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.

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. Microsoft 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.

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

Also referred to as electronic wallets, digital wallets are essentially digital alternatives to a physical wallet. They contain credit and debit card details, like the physical wallet contains cards. A digital wallet allows consumers with a smart device (e.g. mobile phone or tablet) to make purchases on the Internet, or within a shop or store using their device rather than a physical card.

- 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 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.
- 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 you ignore these updates it increases the risk of the device being hacked or compromised.
- Always log out when you have finished using a mobile App.
- Be aware of and ignore emails that request the details and credentials used to log in to your banking App.

ADVICE WHEN USING A MOBILE PHONE CARD READER

Mobile phone card readers are essentially Chip & PIN card readers that use Bluetooth via an App on smart devices (e.g. mobile phones or tablet) or card readers that plug into a mobile phone or tablet. They are increasingly being used by small traders such as plumbers and window cleaners to accept a card payment from their customers.

- Make sure you are dealing with a 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 or card company.

ADVICE WHEN USING MOBILE TO MOBILE PAYMENTS

Mobile to mobile payments allow bank account customers to send and receive payments through their smart device. 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 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 or card company.
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. From September 2015, the contactless card payment limit will increase to £30.
- 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 of 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 passcode (do not 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. (From September 2015, the contactless card payment limit will increase to £30).
- 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, card PINs or credit or debit card details on your mobile phone. These may be compromised, causing you significant inconvenience.
- For added security, passcode protect your smart device. This is the first layer of physical security to protect the contents of the device. In addition to a passcode, 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 passcode.
- 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.
- To protect yourself always try to 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, intending the recipient to believe that it is from their bank. The message usually says someone is trying to send money and asks 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. Try to be aware of what the QR code links to, it may be malicious. Use a QR code reader that allows you to view link addresses after scanning but before visiting the link. 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.
- Always back-up your phone data on a regular basis. Be cautious about utilising ‘cloud’ services for sensitive data.
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: 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.
If you are issued with a new card, fraudsters should not be able to undertake any fraudulent remote purchases (CNP) on your account.
You may consider contacting Cifas 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: 0344 481 0800, www.experian.co.uk
- Equifax: 0845 603 3000, www.equifax.co.uk
- CallCredit: 0845 366 0071, www.callcredit.co.uk
Why did the industry introduce Chip & PIN if contactless technology relies on neither a PIN nor a signature; how are customers authenticated?
Contactless technology is a fast, easy and secure way to pay for goods and services of £20 and under without entering a PIN. Contactless cards have an antenna in the plastic so that when it is used at a contactless card reader it securely transmits information to and from the reader.
Contactless uses secure encryption technology (the same as Chip & PIN) so you can feel confident when using it to pay for items. There is a maximum amount for a contactless transaction of £20 and under. For added protection, from time to time, you may be asked to enter your PIN to verify you are the genuine card holder.
From September 2015, the contactless card payment limit will increase to £30.

I have heard that contactless cards can be copied at a distance by fraudsters using fake card readers. Is this true?
The contactless technology platforms are based on secure chip technology, which protects the data and ensures the transaction is secure by using encryption technology.
A contactless card reader can only interrogate your card when it is within a few centimetres of the card. Also, a contactless card will only release a limited set of data (the same can 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.

In the case of any fraud using a card, cardholders are protected and have the right to a refund for any unauthorised transaction, as long as the card issuer has been notified.

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 and delete all such emails.
Do not correspond with the sender.

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’ or ‘money transfer agents’ launder funds obtained as a result of fraud. They are ordinary people recruited by criminals to help transfer stolen money. Many of the criminals carrying out this type of fraud are located abroad, so a money mule based in the UK is required to send the money overseas. Criminals try to dupe innocent victims into laundering money on their behalf. They normally do this by pretending to offer legitimate jobs via newspapers or the internet, and often target vulnerable groups such as migrant workers or university students who may be tempted by the lure of a seemingly easy way to make extra cash.
Remember that even if you have nothing to do with the actual extraction of funds from another person’s account, by allowing your account to be used to receive and transfer such funds, you will be acting illegally.
Ignorance is no excuse – allowing your bank account to be used for fraud can lead to up to ten years’ imprisonment.
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 is a UK scheme for the electronic processing of financial transactions.

www.bba.org.uk
The BBA is the 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 regulatory agency in the UK, and their aim is to protect consumers, ensure the Industry remains stable and to promote healthy competition between financial service providers.

www.financialfraudaction.org.uk
Financial Fraud Action UK (FFA UK) is responsible for leading the collective fight against fraud in the UK payments industry. Our membership includes banks, credit, debit and charge card issuers, and card payment acquirers in the UK. We provide a forum for our members to work together on non-competitive issues relating to financial fraud. Our primary function is to facilitate collaborative activity between industry participants and with other partners.

www.financial-ombudsman.org.uk
Provides assistance in resolving complaints against any 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.payyourway.org.uk
Pay Your Way is a payments industry website set up to provide impartial information for customers 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 telecommunications UK Fraud 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.
Financial Fraud Action UK
2 Thomas More Square
London, E1W 1YN

www.financialfraudaction.org.uk

Financial Fraud Action UK
@FFA UK

Printed on paper made from well managed sources containing 100% recycled chlorine free material. Cover laminated with Cellogreen which is sustainable, compostable and recyclable.

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 Financial Fraud Action UK 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.

© Financial Fraud Action UK Ltd 2015. Published by Financial Fraud Action UK Ltd.