Financial Fraud Action UK
Working together to prevent fraud

UK FINANCE

2017 half year fraud update:

Payment cards, remote banking and cheque

September 2017

Fraud is always evolving, but the industry takes the threat extremely seriously and continuously reviews and reinvests in detection and verification systems to protect customers and stop fraud.

In the first half of 2017, losses due to financial fraud fell by 8 per cent. However, we know that criminals continue in their attempts to circumvent banks' security systems by using a range of tactics to steal customers' personal and security information.

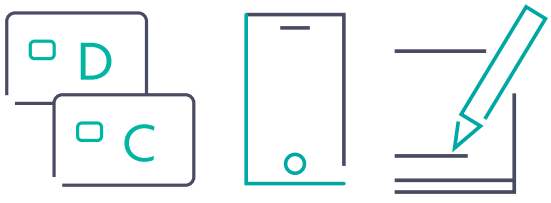
The finance industry is responding by:

- Further investing in the Take Five to Stop Fraud Campaign in conjunction with the Home Office, to raise awareness of fraud and scams and explain how customers can protect themselves
- Working with law enforcement and government through the Joint Fraud Taskforce to use our collective powers to combat fraud and protect customers
- Introducing new procedures between police and bank branches to prevent vulnerable people from falling victim to fraud, exploring new ways to track stolen funds moved between multiple bank accounts, and creating new standards setting out how customers reporting cases of fraud are handled
- Sharing intelligence about the latest threats through Financial Fraud Action UK's fraud intelligence hub
- Fully-sponsoring a dedicated police unit which targets the criminals responsible for fraud.

To stay safe, customers are urged to follow the advice of our Take Five campaign:

- A genuine bank or organisation will never contact you asking for your PIN, full password or to move money to a safe account.
- Never give out personal or financial information. Always contact the company directly using a known email or phone number.
- Don't be tricked into giving a fraudster access to your details. Never automatically click on a link in an unexpected email or text.
- Always question uninvited approaches, in case it's a scam.

This update covers latest card, remote banking and cheque fraud losses.



Fraud: January to June 2017

Total financial fraud	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/ H1 17 %
Pre-vented Value	N/A	N/A	N/A	N/A	£939.5m	£821.5m	£678.7m	£708.9m	£751.4m	11%
Cases	595,855	665,928	687,080	631,119	610,225	816,019	937,274	920,232	937,518	0%
Gross Loss	£264.7m	£288.6m	£306.9m	£290.6m	£320.3m	£435.3m	£400.4m	£516.5m	£366.4m	-8%

Every 15 seconds, someone is defrauded in the UK.

Financial fraud losses across payment cards, remote banking and cheques totalled £366.4 million in January to June 2017, a decrease of 8 per cent compared to the same period in 2016.

- There were 937,518 cases of financial fraud during the first six months of this year, a figure that has remained flat compared with the year before
- Prevented fraud totalled £751.4 million in the first half of 2017. This represents incidents that were detected and prevented by banks and card companies and is equivalent to £6.72 in every £10 of attempted fraud being stopped
- The proportion of prevented fraud has increased from £6.29 in every £10 in the first half of 2016.

What's driving the fraud losses?

Fraudsters use a wide range of tactics. While it is not possible to be more specific about the values that can be attributed to individual methods, intelligence from our members highlights the main drivers.

In the first half of 2017, criminals' use of compromised personal and financial details continued to be a key driver of fraud losses. Customer details are primarily stolen through online attacks, such as data hacks and malware, as well as through impersonation scams.

Over two thirds of financial fraud is prevented by the industry.

In an impersonation scam, fraudsters contact customers by phone, email or text message pretending to represent a trusted organisation, such as a bank, the police, a utility company or a government department. Often the approach claims there has been suspicious activity on an account, account details need to be 'updated' or 'verified', or a refund is due. The criminal then attempts to trick their intended victim into giving away their personal or financial information, such as passwords, card and bank account details, or into allowing remote access to their computer.

Recent intelligence suggests that criminals are increasingly using scam text messages to trick customers into giving away details and clicking on links. At the same time, fraudsters are sending phishing emails purporting to be from major online retailers and internet companies, which many customers use.

Data breaches continue to be a major contributor to fraud losses. Stolen data may be used to commit fraud directly, for example card details are used to make online purchases. Criminals also use personal and financial information obtained in a breach to target individuals in impersonation scams, while the publicity around the incident itself can be used to add authenticity to a fraudulent approach.

Intelligence also suggests there continues to be a rise in distraction thefts and card entrapment at ATMs, with fraudsters obtaining both the card and the PIN. This enables them to commit fraud at cash machines and in stores.

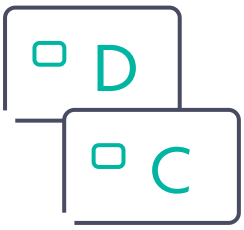
Our fraud data

Financial Fraud Action UK publishes both the value of fraud losses and the number of cases. The data is reported to us by our members which include financial providers, credit, debit and charge card issuers, and card payment acquirers.

Each incident of fraud does not equal one person being defrauded, but instead refers to the number of cards or accounts defrauded. For example, if a fraud was carried out on two cards, but they both belonged to the same person, this would represent two instances of fraud, not one.

All fraud loss figures, unless otherwise indicated, are reported as gross. This means the figures represent the total value of fraud including any money subsequently recovered by a bank.

Debit and credit and other payment card fraud



Total UK-issued payment card fraud	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/ H1 17 %
Prevented value	N/A	N/A	N/A	N/A	£366.3m	£477.3m	£475.7m	£510.3m	£502.4m	6%
Loss value	£216.1m	£234.1m	£247.6m	£231.4m	£244.6m	£323.5m	£321.5m	£296.5m	£287.3m	-11%
Number of cases	581,005	650,912	671,388	616,824	593,417	793,775	917,479	903,247	917,686	0%

Total UK-issued payment card fraud

This covers fraud on debit, credit, charge and ATM-only cards issued in the UK.

Payment card fraud losses are organised into five categories: remote card purchase, lost and stolen, card not received, counterfeit card and card ID theft.

Fraud losses on cards totalled £287.3 million in January to June 2017, a decrease of 11 per cent on the same period in 2016.

Over this period, overall card spending grew by 8.4 per cent. Card fraud as a proportion of card purchases is therefore 7.5p for every £100 spent, down from 8.7p at the end of H1 2016.

A total of £502.4 million of card fraud was stopped by banks and card companies in the first half of 2017, a rise of 6 per cent on 2016. This is equivalent to £6.36 in every £10 of attempted card fraud being prevented.

The finance industry is tackling card fraud by:

- Investing in new, innovative security tools, including even more sophisticated ways of authenticating customers
- Providing fraud screening detection tools for retailers such as the continued growth in the use of 3D Secure technology which protects purchases by card over the internet
- Speedily, safely and securely identifying compromised card details through FFA UK's intelligence hub so that card issuers can put protections in place
- Working with government and law enforcement in the Joint Fraud Taskforce to use our collective powers, systems and resources to crack down on financial fraud
- Fully-sponsoring a specialist police unit, the Dedicated Card and Payment Crime Unit, which targets organised criminals responsible for card fraud.

Remote card purchase fraud

Remote purchase fraud	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/ H1 17 %
Loss value	£142.0m	£159.1m	£174.5m	£157.0m	£171.7m	£226.7m	£224.1m	£208.2m	£205.5m	-8%
Number of cases	443,164	508,834	537,302	481,844	473,504	639,580	728,087	709,745	704,465	-3%

This fraud occurs when a criminal uses stolen card details to buy something on the internet, over the phone or through mail order. It is also referred to as card-not-present (CNP) fraud.

Losses due to remote purchase fraud fell by 8 per cent to £205.5 million in the first half of 2017.

Intelligence suggests remote purchase fraud continues to result mainly from criminals using card details stolen through data hacks, via phishing emails, and text messages.

Contained within these figures, e-commerce card fraud totalled an estimated £154.5 million in H1 2017, down 1 per cent compared to the first half of 2016.

Remote purchase fraud: E-commerce / Mail order and telephone order	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/ H1 17 %
E-commerce	£96.5m	£108.0m	£118.5m	£100.6m	£107.2m	£154.2m	£156.4m	£152.4m	£154.5m	-1%
Mail and telephone order	£45.5m	£51.1m	£56.0m	£56.4m	£64.4m	£72.5m	£67.7m	£55.8m	£51.0m	-25%

How to stay safe from this fraud:

- If you're using a retailer for the first time, always take time to research them before you give them any of your details. Be prepared to ask questions before making a payment
- Trust your instincts – if an offer looks too good to believe then it probably is. Be suspicious of prices that are too good to be true
- Look for the padlock symbol in the web address bar. It's a good indication that a retailer is reputable
- Only use retailers you trust, for example ones you know or have been recommended to you. If you're buying an item made by a major brand, you can often find a list of authorised sellers on their official website.

Lost and stolen fraud

Lost and stolen fraud	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/ H1 17 %
Loss value	£28.2m	£30.6m	£29.2m	£30.5m	£30.3m	£43.8m	£49.5m	£46.8m	£47.8m	-3%
Number of cases	65,266	73,701	66,218	67,725	61,500	82,302	109,110	122,054	148,554	36%

This fraud occurs when a criminal uses a lost or stolen card to make a purchase (whether remotely or face-to-face), takes money out at an ATM or in a branch or makes a payment from one card to another. Losses due to lost and stolen fraud fell by 3 per cent in the first half of 2017 to £47.8 million. The number of incidents increased by 36 per cent, indicating a lower loss value per individual case as bank systems detected fraudulent spending on a lost or stolen card more quickly.

Intelligence suggests a major cause of lost and stolen fraud is distraction thefts and card entrapment at ATMs, with fraudsters obtaining both the card and the PIN enabling them to commit fraud at cash machines and in stores.

How to stay safe from lost and stolen fraud:

- Always report any lost or stolen cards to your bank or card company straight away
- Make sure you fully cover your PIN with your free hand or purse whenever you enter it
- If you spot anything suspicious with an ATM, or someone is watching you, then do not use the machine and report it to your bank
- Check your statements regularly and if you spot any payments you don't recognise then contact your card company immediately.

Card not received fraud

Card not received fraud	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/ H1 17 %
Loss value	£4.6m	£5.8m	£5.0m	£5.0m	£5.7m	£5.9m	£6.1m	£6.4m	£5.5m	-10%
Number of cases	4,278	4,847	4,366	4,936	5,033	5,686	5,685	5,692	5,479	-4%

This type of fraud occurs when a card is stolen in transit, after a card company sends it out but before the genuine cardholder receives it.

Card not received fraud losses fell by 10 per cent in the first half of 2017 to £5.5 million. To commit this fraud, criminals often target multi-occupancy buildings, such as flats, where post is not securely stored.

How to stay safe from this fraud:

- If you are expecting a new card and it hasn't arrived, then call your bank or card company for an update
- Tell your bank or card issuer immediately if you move home. Ask Royal Mail to redirect your post to your new home for at least a year
- Be extra careful if you live in a property where other people have access to your mail such as a block of flats. In some cases your card company may arrange for you to collect your cards from a local branch.

Counterfeit card fraud

Counterfeit card fraud	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/ H1 17 %
Loss value	£23.3m	£20.0m	£24.1m	£23.7m	£19.8m	£25.9m	£21.3m	£15.7m	£12.7m	-40%
Number of cases	53,653	47,456	49,924	49,355	39,711	46,310	58,268	50,329	43,431	-25%

This fraud occurs when a fake card is created by a fraudster using compromised details from the magnetic stripe of a genuine card. This typically occurs because of criminals using a device to steal details from a UK-issued card at an ATM or unattended payment terminal, such as at a car park. A fake magnetic stripe card is then created to be used overseas in countries yet to upgrade to chip & PIN.

Counterfeit card fraud losses fell by 40 per cent to £12.7 million in the first half of 2017. This fall is likely due to the increased rollout of chip technology around the world, particularly in the US.

How to stay safe from counterfeit card fraud:

- Always protect your PIN by fully covering the keypad with your free hand or purse
- If you spot anything suspicious at an ATM or unattended terminal, or someone is watching you, then do not use the machine and report it to your bank
- Check your statements regularly and if you spot any payments you don't recognise then contact your card company immediately.

Card ID theft

Card ID theft	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/ H1 17 %
Loss value	£18.1m	£18.6m	£14.7m	£15.2m	£17.1m	£21.1m	£20.5m	£19.5m	£15.7m	-24%
Number of cases	14,644	16,074	13,578	12,964	13,669	19,897	16,329	15,427	15,757	-4%

Card ID theft occurs in two ways, through third-party applications or account takeover.

Third-party application fraud happens when a criminal uses stolen or fake documents to open an account in someone else's name.

Account takeover occurs when a criminal takes over another person's genuine card account. The criminal will gather information about the intended victim, often through impersonation scams, before contacting the bank or card issuer masquerading as the genuine cardholder.

Third party applications accounted for £5.6 million of card ID theft during the first half of 2017, down 34 per cent from £8.6 million in H1 2016. Account take-over accounted for £10.1 million of card ID theft, down 16 per cent from £12.0 million in the first half of 2017.

How to stay safe from card ID fraud:

- Don't be tricked into giving a fraudster access to your personal or financial information
- Never automatically click on a link in an unexpected email or text and always question uninvited approaches
- Look after your personal documents – keep them secure at home and rip up any bills or statements before you throw them away
- Check your credit record for any applications you don't recognise. You can do this by contacting a credit reference agency.

Further card fraud analysis

Figures in the following sections relate to the places where the card was fraudulently used, rather than how the card or card details were compromised.

These figures are another way of breaking down the overall payment card fraud totals and are not in addition to those covered previously. Case volumes are not available for the place of misuse as one case can cover multiple places of misuse. This can lead to double counting. For example, a lost or stolen card could be used to make an ATM withdrawal and to purchase goods on the high street.

UK retail face-to-face card fraud

UK retail face-to-face fraud	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/ H1 17 %
Loss value	£27.3m	£29.9m	£25.6m	£23.7m	£23.0m	£30.6m	£31.8m	£31.0m	£31.2m	-2%

UK retail face-to-face fraud covers all transactions that occur in person in a UK shop.

Most of this fraud takes place using cards obtained through more basic techniques, with fraudsters finding ways of stealing both the card and PIN to carry out fraudulent transactions in shops. This includes criminals targeting cards and PINs through distraction thefts and entrapment devices at ATMs combined with shoulder surfing or PIN pad cameras. Criminals also use methods to dupe victims into handing over their cards on their own doorstep.

Contactless fraud covers fraud on both contactless cards and mobile devices. Fraud on contactless cards and devices remains low with £5.6 million of losses during the first half of 2017, compared to spending of £23.23 billion over the same period.

This is equivalent to 2.4p in every £100 spent using contactless technology and is a decrease on the same period in 2016 when it was 3.1p in every £100. Fraud on contactless cards and devices represents just 1.9 per cent of overall card fraud.

UK cash machine fraud

UK cash machine fraud	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/H1 17 %
Loss value	£16.2m	£15.7m	£14.3m	£13.0m	£14.9m	£17.8m	£20.6m	£22.5m	£20.5m	0%

These figures show how much fraud took place at cash machines in the UK using a compromised card. In all cases the fraudster would need to have access to the genuine PIN and card.

Losses at UK cash machines remained steady at £20.5 million in the first half of 2017.

Intelligence suggests much of this fraud is due to distraction thefts and card entrapment at ATMs, with fraudsters obtaining both the card and the PIN which enables them to make fraudulent cash withdrawals.

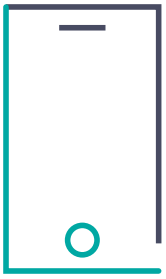
Domestic and international card fraud

Domestic / International split	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/ H1 17 %
UK fraud	£155.9m	£172.4m	£175.1m	£153.6m	£164.6m	£215.1m	£215.2m	£202.7m	£205.3m	-5%
International fraud	£60.2m	£61.8m	£72.5m	£77.8m	£80.1m	£108.4m	£106.3m	£93.9m	£82.0m	-23%

These figures provide a breakdown of fraud committed on a UK issued credit, debit or charge card split between UK or international fraud spending location.

Intelligence suggests that much of the decline in international fraud is due to the roll out of chip and PIN technology around the world.

Remote banking fraud



Total remote banking fraud	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/ H1 17 %
Prevented Value	N/A	N/A	N/A	N/A	£311.3m	£213.3m	£103.2m	£102.2m	£160.2m	55%
Loss value	£31.7m	£40.1m	£47.3m	£51.0m	£66.2m	£102.4m	£71.5m	£65.6m	£73.8m	3%
Number of cases	9,566	9,829	10,908	10,911	13,971	19,335	17,687	15,705	18,848	7%

Remote banking fraud losses are collated in three categories: internet, phone and mobile banking. It occurs when the fraudster gains access to an individual's bank account and transfers money out of it.

Remote banking fraud totalled £73.8 million in the first half of 2017, a 3 per cent rise from £71.5 million in January to June 2016.

A total of £160.2 million of attempted remote banking fraud was stopped by bank security systems during the first half of the year. This is equivalent to £6.84 in every £10 of fraud attempted being prevented.

The proportion of prevented fraud has risen from £5.91 in every £10 during the same period in 2016.

In addition, 22 per cent (£16.4 million) of the losses across all remote banking channels were recovered after the incident.

The finance industry is tackling remote banking fraud by:

- Investing in new, innovative security tools, including ever more sophisticated ways of authenticating customers, such as using biometrics and customer behaviour analysis
- Providing customers free security software, which many banks offer
- Investing in the Take Five to Stop Fraud campaign to educate customers on how they can protect themselves from fraud
- Sharing intelligence and information on this type of fraud so that security systems can be adapted to stop the latest threats
- Working with law enforcement, the telecommunications industry and other key stakeholders to further improve security and to identify and prosecute the perpetrators.

Internet banking fraud

Internet banking fraud	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/ H1 17 %
Loss value	£25.5m	£33.3m	£39.9m	£41.6m	£50.4m	£83.1m	£56.1m	£45.6m	£55.5m	-1%
Number of cases	6,770	7,029	8,150	7,891	8,417	11,274	11,195	8,893	11,725	5%

This type of fraud occurs when a fraudster gains access to a customer's online bank account and transfers money from it.

This is typically done by fraudsters tricking customers into revealing their security details through scam phone calls, texts and email, or details obtained through malware, which are then used to access a customer's online account.

Losses due to internet banking fraud fell by 1 per cent in the first half of 2017 to £55.5 million, while the number of cases increased by 5 per cent.

In addition, 23 per cent (£12.7 million) of the losses across internet banking were recovered after the incident.

How to stay safe from internet banking fraud:

- Don't be tricked into giving a fraudster access to your personal or security details
- Never automatically click on a link in an unexpected email or text and always question uninvited approaches
- Remember that your bank or the police will never call you to ask for you full online banking password
- Ensure you have the most up-to-date security software installed on your computer, including anti-virus. Some banks offer free security software so check your bank's website for details.

Telephone banking fraud

Telephone banking fraud	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/H1 17 %
Loss value	£6.2m	£6.9m	£7.4m	£9.4m	£14.7m	£17.6m	£13.1m	£16.5m	£15.6m	19%
Number of cases	2,796	2,800	2,758	3,020	4,777	6,603	4,949	5,546	5,273	7%

This fraud occurs when a fraudster gains access to a customer's phone banking account and transfers money from it.

Losses due to phone banking fraud rose totalled £15.6 million in the first half of 2017, a 19% rise on the same period in 2016.

In addition, 19 per cent (3.0million) of the losses across telephone banking were recovered after the incident.

Intelligence suggests that criminals have shifted their focus away from using malware which targets online banking systems, to using compromised details to take money from accounts using the telephone banking service.

How to stay safe from phone banking fraud:

- Never disclose security details, such as your full banking password. A genuine financial provider or organisation will never ask you for these in an email, on the phone or in writing
- Don't assume the person on the phone is who they say they are. Just because someone knows your basic details (such as your name and address or even your mother's maiden name), it doesn't mean they are genuine.

Mobile banking fraud

Mobile banking fraud	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/ H1 17 %
Loss value	N/A	N/A	N/A	N/A	£1.0m	£1.8m	£2.2m	£3.5m	£2.6m	19%
Number of cases	N/A	N/A	N/A	N/A	777	1,458	1,543	1,266	1,850	20%

These are fraudulent payments or attempts made via mobile banking services accessed only through a banking app downloaded to a mobile device. It also includes any frauds made via an SMS payment but excludes mobile web browser banking and browser based banking apps.

Losses due to mobile banking fraud totalled £2.6 million in the first half of 2017, a 19 per cent rise on the same period in 2016. The rise in fraud reflects the growing number of customers using mobile banking and a larger offering of mobile banking facilities by banks.

In addition, 23 per cent (£0.6 million) of the losses across mobile banking were recovered after the incident.

How to stay safe from mobile banking fraud:

- Don't be tricked into giving a fraudster access to your personal or security details. Never automatically click on a link in an unexpected email or text and always question uninvited approaches
- Be wary of text messages that encourage you urgently to visit a website or call a number to verify or update your details.

Cheque fraud

Telephone banking fraud	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H1 16/ H1 17 %
Total prevented value	£198.5m	£221.7m	£212.1m	£216.8m	£262.0m	£130.9m	£99.8m	£96.4m	£88.8m	-11%
Total loss value	£16.9m	£14.4m	£12.0m	£8.2m	£9.5m	£9.4m	£7.4m	£6.3m	£5.3m	-28%
Total number of cases	5,284	5,187	4,784	3,384	2,837	2,909	2,108	1,280	984	-53%

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

Counterfeit cheques are printed on non-bank paper to look exactly like genuine cheques and are drawn by a fraudster on genuine accounts.

Forged cheques are genuine cheques that have been stolen from an innocent customer and used by a fraudster with a forged signature.

A fraudulently altered cheque is a genuine cheque that has been made out by the genuine customer, but has been altered in some way by a fraudster before it is paid in, e.g. by changing the beneficiary's name or the amount of the cheque.

Cheque fraud losses fell to £5.3 million in the first half of 2017, a 28 per cent drop on the same period in 2016. This is the lowest half year total ever reported.

A total of £88.8 million of cheque fraud was prevented by bank monitoring systems in the first half of 2017. This is equivalent to £9.44 in every £10 of attempted cheque fraud being stopped before a loss occurs.

How to stay safe from cheque fraud:

- Always complete cheques using a ballpoint pen, or pen with indelible ink
- Draw a line through all unused spaces, including after the payee name
- Keep your chequebook in a safe place, report any missing cheques to your bank immediately and always check your bank statement thoroughly.

Some caveats are required for the tables in the document.

- *Prevented values where not collected for all fraud types prior to 2015.*
- *Sum of components may not equal the total due to rounding.*

The Take Five to Stop Fraud campaign was devised by Financial Fraud Action UK to help fight fraud. www.takefive-stopfraud.org.uk

If you have any questions about this report please contact the press team: press@ukfinance.org.uk

For general information about payments and UK Finance please contact External Affairs: info@ukfinance.org.uk