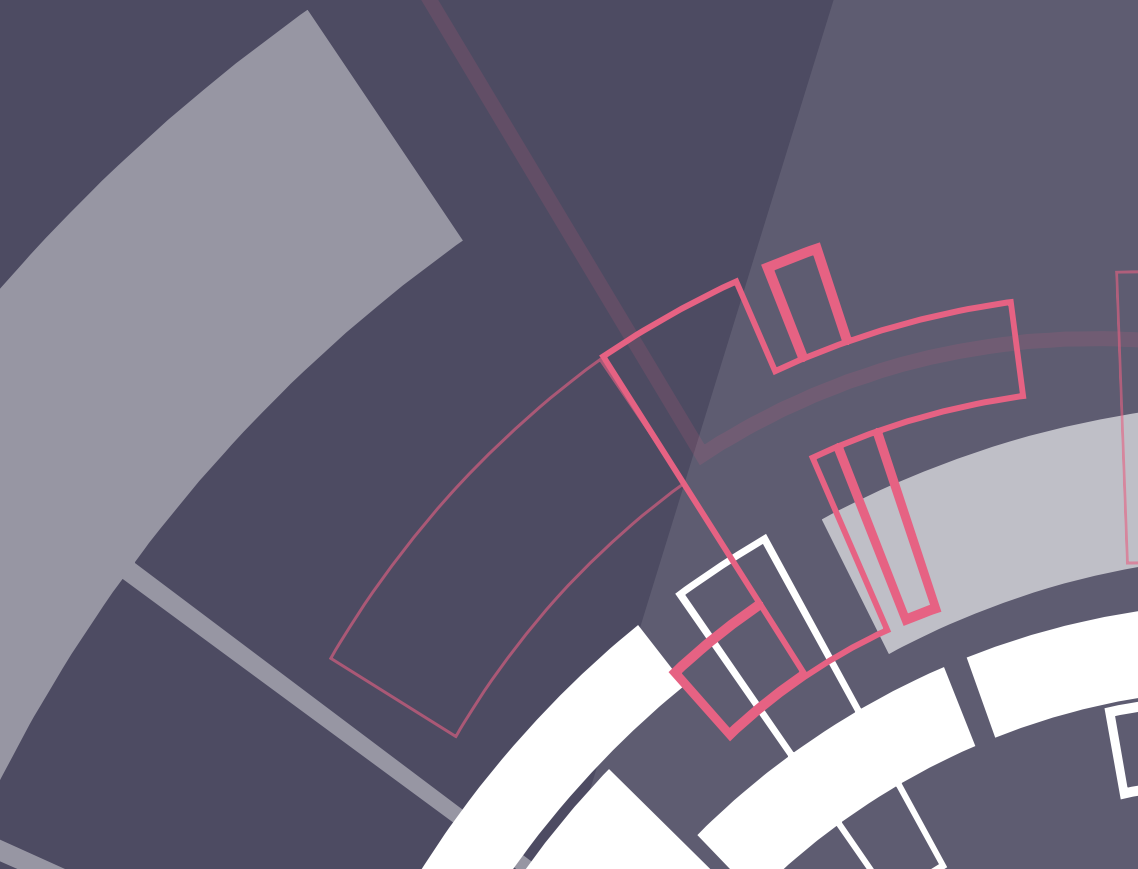
UK FINANCE

Fraud the Facts 2018

The definitive overview of payment industry fraud



Financial Fraud Action (FFA UK) is now part of UK Finance, which was launched on 1st July 2017. UK Finance drives collaborative action to reduce the impact of financial fraud and scams both across the industry and with partners in the public sector, private sector and law enforcement, operates its own data and intelligence sharing bureau and sponsors a fully operational police unit.

KEY ACTIVITIES:

- Managing the industry strategic threat management process, which provides an up-to-the-minute picture of the threat landscape
- Sponsoring the Dedicated Card and Payment Crime Unit (DCPCU), a unique proactive operational police unit with a national remit, formed as a partnership between UK Finance, the City of London Police, and the Metropolitan Police
- Managing intelligence-sharing through the industry intelligence hub (Financial Fraud Bureau) and the Fraud Intelligence Sharing System (FISS) which feed intelligence to police and other agencies in support of law enforcement activity
- Providing a single point of contact for companies suffering data breaches, to ensure compromised account information can be speedily, safely and securely repatriated to the banks
- Delivering UK-wide awareness campaigns to inform customers about threats and how to stay safe
- Informing commentators and policymakers through press office and public affairs functions
- 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

CONTENTS

INTRODUCTION

The threat from fraud is ever changing. Fraud the Facts 2018 shows the extent and nature of the challenge faced – and one which the finance industry is committed to tackling.

The financial services industry invest millions of pounds every year in advanced security systems to root out fraud. In 2017, £2 in every £3 of unauthorised fraud was stopped. That means a total of over £1.4 billion was prevented from falling into the hands of criminals. This is money that would probably have gone on to fund further criminal acts such as terrorism, drug trafficking and people smuggling.

As the data in this report shows, we know there is still more to do. Losses due to unauthorised financial fraud fell five per cent last year, totalling almost £732 million. However this, figures collated for the first time on authorised push payment (APP) scams show an additional £236 million was stolen last year.

In 2017 the industry introduced new standards to ensure those who have fallen victim to fraud or scams get the help they need [and all banks are working towards the introduction of suitably trained staff available 24-hours, 7-days-a-week to deal with and process APP scam complaints]. At the same time, UK Finance continues to work with the government and law enforcement through the Joint Fraud Taskforce to deter and disrupt criminals and better trace, freeze and return stolen funds.

To help protect customers, we have developed initiatives such as the Banking Protocol – a ground-breaking rapid response scheme through which branch staff can alert police and Trading Standards to suspected frauds taking place. In 2017, while the Protocol was being rolled out to police forces across the country, it prevented £13.3 million of fraud and led to 129 arrests.

Criminals are increasingly directly targeting individuals and businesses for their data and money, using social engineering tactics to commit their crimes. Through this method fraudsters pose as legitimate organisations and manipulate people into revealing their details or parting with their money. Through the Take Five to Stop Fraud campaign, led by UK Finance and backed by government, we are helping people to confidently challenge such approaches and stay safe.

Fraud is an issue that affects the whole of society, and one which everyone must come together to tackle. The fact is financial services industry can't stop all fraud on its own. We all need to work together across the public and private sector, because as a combined force we can stamp out fraud and the criminals behind it.

KATY WOROBEC
Managing Director:
Economic Crime, UK Finance

TRENDS AND STATISTICS

Unauthorised financial fraud losses across payment cards, remote banking and cheques totalled £731.8 million in 2017, a decrease of five per cent compared to 2016.

In 2017 the financial services industry prevented unauthorised fraud totalling £1.46 billion equivalent to £2 in every £3 of attempted fraud being stopped.

For the first time UK Finance published data for authorised push payment (APP) scams. This data has never been collected before and was not previously included in any other reporting category. In 2017 UK Finance members reported 43,875 incidents of APP scams with gross losses of £236 million.

Drivers of the changing fraud figures

Fraudsters use a wide range of tactics. While it is not possible to place specific monetary values on particular methods used, intelligence reported by our members indicates the key drivers behind the reported figures.

In 2017, criminals' use of social engineering tactics through deception and impersonation scams continued to be a key driver of both unauthorised and authorised fraud losses. Social engineering – in relation to financial fraud – is a method through which criminals manipulate people into divulging personal or financial details, or into transferring money directly to the them.

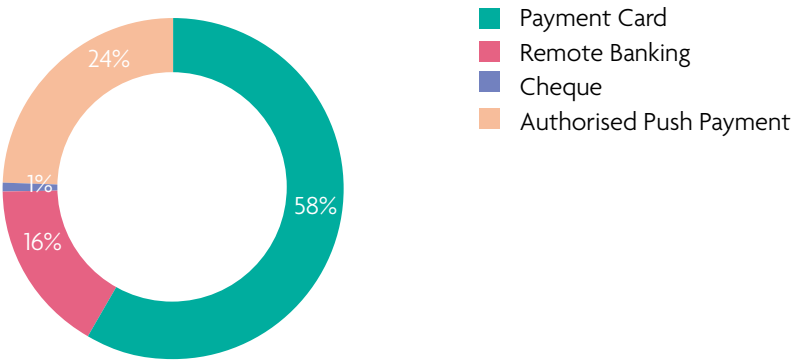
In an impersonation scam, fraudsters contact customers by phone, text message or email pretending to represent a trusted organisation, such as a bank, the police, a utility company or a government department. Often the approach claims there has been suspicious activity on an account, account details 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 and passcodes, card and bank account details, or into allowing remote access to their computer.

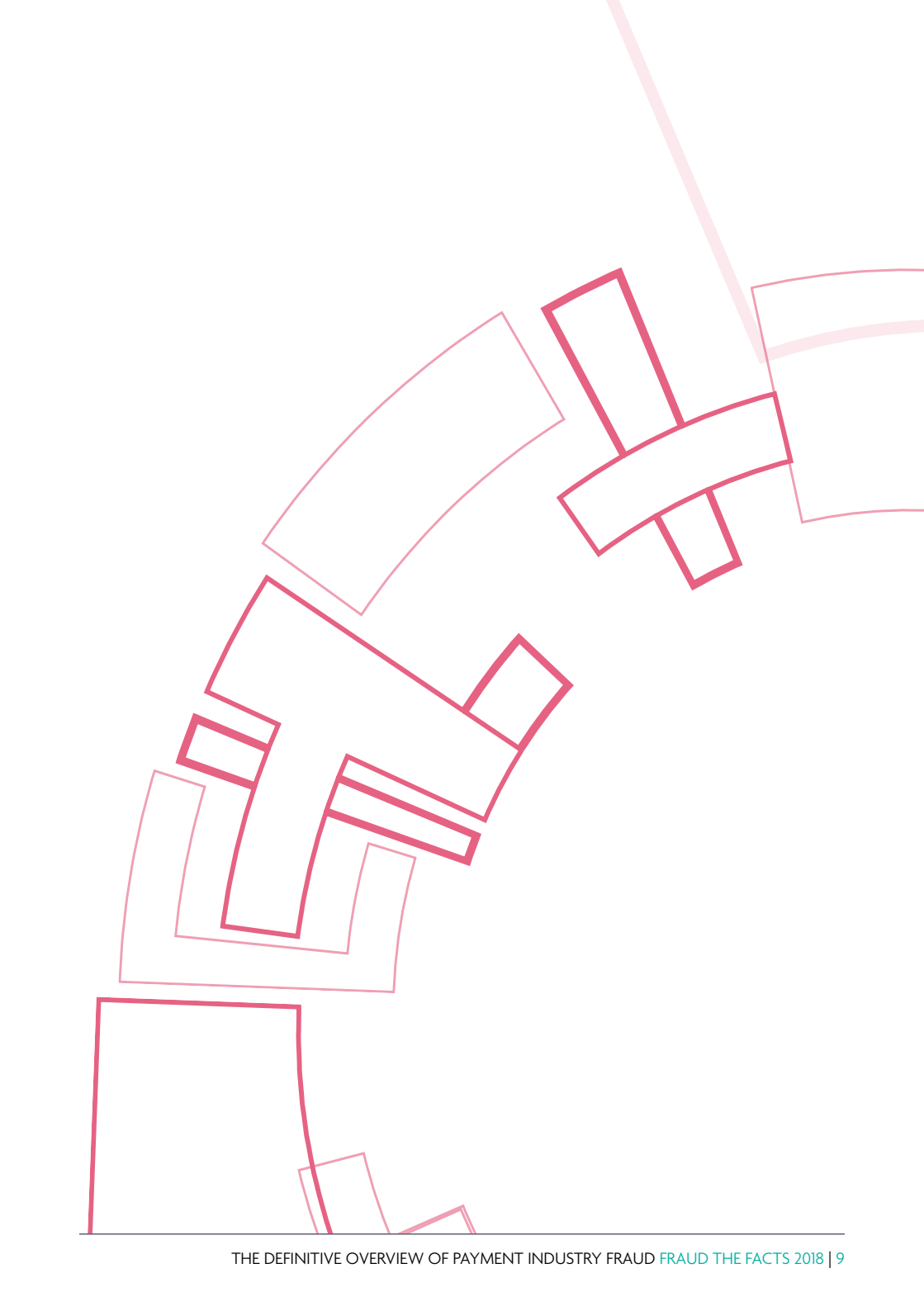
This information is then used by the criminal to make an unauthorised payment. Criminals also use these fraudulent approaches to trick people into authorising a payment to them. Fraudsters use a range of tactics to commit this crime, including impersonating someone from a bank, or a police officer, claiming a fraud has been spotted on a customer's account and that money needs to be transferred to a 'safe account'; sending fake invoices to businesses; offering fraudulent investment opportunities; and online auction scams.

Data breaches also continue to be a major contributor to fraud losses. Criminals use stolen data to commit fraud directly, for example, card details are used to make unauthorised purchases online or personal details used to apply for credit cards. Stolen personal and financial information is also used by criminals to target individuals in impersonation and deception scams and can add apparent authenticity to their approach.

Intelligence also suggests criminals are using more low-tech methods such as distraction thefts and card entrapments to steal debit and credit cards which are then used to commit fraud.

Total 2017 financial fraud losses by type





CARD FRAUD

VALUE	£566.0m	(-8%)

VOLUME	1,874,002	(+3%)

Fraud losses on UK-issued cards totalled £566.0 million in 2017, an eight per cent decrease from £618.1 million in 2016; the first decrease reported in six years. At the same time, total spending on all debit and credit cards reached £755 billion in 2017, with 18.3 billion transactions made during the year.

Overall card fraud losses as a proportion of the amount we spend on our cards decreased during 2017, falling from 8.3p per £100 spent in 2016 to 7.0p per £100 in 2017 (in 2008 it was 12.4p for every £100 spent).

The finance industry is tackling card fraud by:

- Investing in new, innovative security tools to identify suspicious transactions, including even more sophisticated ways of authenticating customers
- Providing fraud screening detection tools for retailers, such as the continued development of 3D Secure technology which protects card purchases online
- Speedily, safely and securely identifying compromised card details through UK Finance'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 (DCPCU), which targets organised criminal groups responsible for card fraud

Fraud volumes

UK Finance also publishes the number of fraud incidents to convey more fully the dynamics of the fraud environment in the UK. There was a significant rise in lost and stolen cases in 2017 which has driven the increase overall. However, lost and stolen gross losses have fallen four per cent whilst case volumes have grown 51 per cent, indicating that lost and stolen cases are being spotted and stopped by card issuers before significant losses have occurred.

Annual case volumes on UK-issued cards 2012 – 2017

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

CARD FRAUD TYPE ON UK-ISSUED CREDIT AND DEBIT CARDS	2012	2013	2014	2015	2016	2017	% CHANGE 16/17
Remote Purchase (CNP)	752,450	951,998	1,019,146	1,113,084	1,437,832	1,399,031	-3%
Counterfeit (skimmed/cloned)	98,555	101,109	99,279	86,021	108,597	84,861	-22%
Fraud on lost or stolen cards	113,162	138,967	133,943	143,802	231,164	350,066	51%
Card ID theft	24,287	30,718	26,542	33,566	31,756	29,139	-8%
Card non-receipt	9,053	9,125	9,302	10,719	11,377	10,905	-4%
TOTAL	997,507	1,231,917	1,288,212	1,387,192	1,820,726	1,874,002	3%

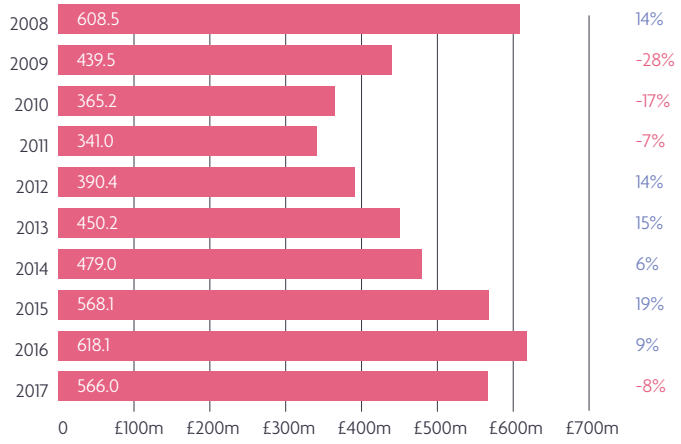
Annual fraud losses on UK-issued cards 2008 - 2017

All figures in £ millions

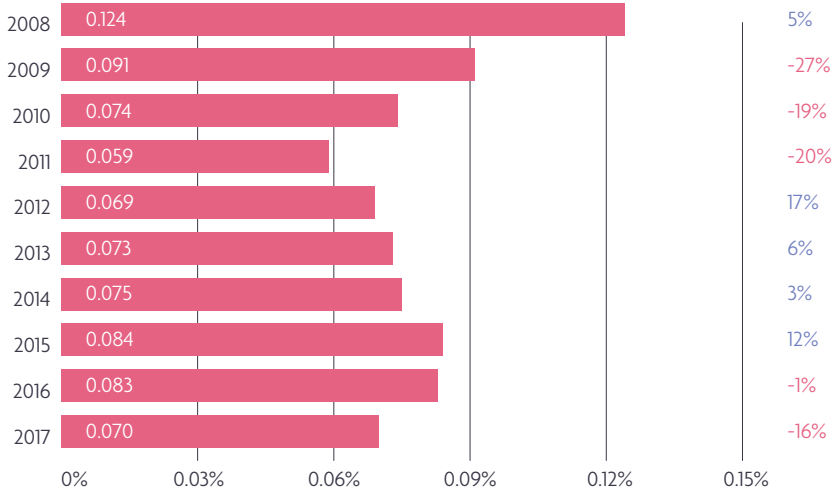
FRAUD TYPE	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	% CHANGE 16/17
Remote Purchase (Card Not Present)	328.4	266.4	226.9	221.0	247.3	301.0	331.5	398.4	432.3	409.4	-5%
Of which e-commerce	181.7	153.2	135.1	139.6	140.2	190.1	219.1	261.5	310.3	310.2	0%
Counterfeit	169.8	80.9	47.6	36.1	42.3	43.3	47.8	45.7	36.9	24.2	-35%
Lost & Stolen	52.7	47.2	44.2	50.1	55.4	58.9	59.7	74.1	96.3	92.5	-4%
Card ID Theft	47.4	38.1	38.1	22.5	32.6	36.7	30.0	38.2	40.0	29.9	-25%
Card non-receipt	10.2	6.9	8.4	11.3	12.8	10.4	10.1	11.7	12.5	10.1	-19%
TOTAL	608.5	439.5	365.2	341.0	390.4	450.2	479.0	568.1	618.1	566.0	-8%
UK	378.4	317.0	271.4	260.9	288.4	328.3	328.7	379.7	417.9	407.6	-2%
Fraud Abroad	230.1	122.6	93.9	80.0	102.0	122.0	150.3	188.4	200.2	158.4	-21%

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

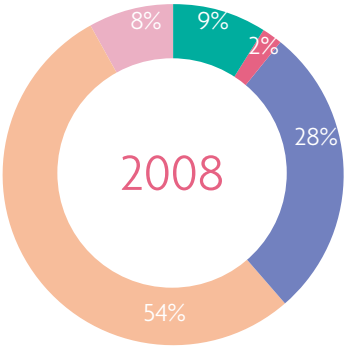
Fraud losses on UK-issued cards 2008-2017 (gross)

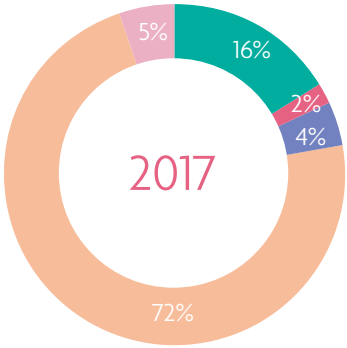


Fraud to turnover ratio 2008 - 2017



Card fraud losses 2017 split by type (as a percentage of total losses)





- Lost & Stolen
- Card not received
- Counterfeit card
- Remote Purchase (CNP)
- Card ID Theft

- Lost & Stolen
- Card not received
- Counterfeit card
- Remote Purchase (CNP)
- Card ID Theft

REMOTE PURCHASE (CARD-NOT-PRESENT) FRAUD

(internet, telephone, mail order)

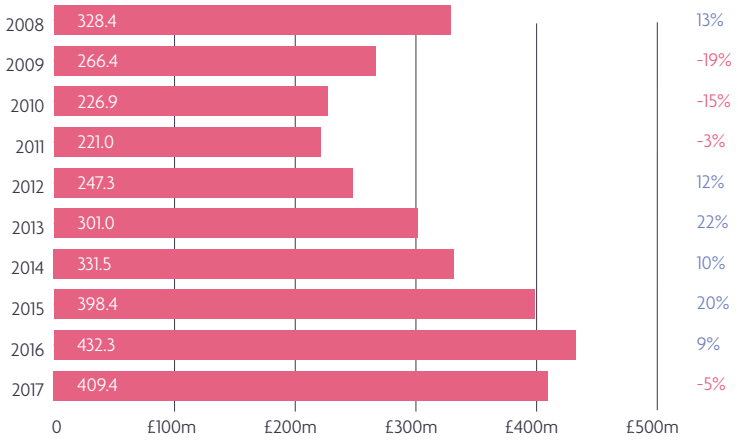
VALUE	£409.4m	(-5%)

VOLUME	1,399,031	(-3%)

The clear majority of this type of fraud involves the use of card details that have been fraudulently obtained through methods such as unsolicited emails or telephone calls, or via digital attacks such as malware and data hacks. 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.

E-commerce fraud against UK retailers totalled an estimated £206.0 million in 2017, a rise of eight per cent on the previous year. However, mail and telephone order (MOTO) fraud against retailers based in the UK reduced significantly, falling 13 per cent to £81.6 million in 2017. Overall card-not-present fraud fell to £409.4mn in 2017; a reduction of five per cent when compared to 2016.

Remote purchase (CNP) fraud losses on UK-issued cards 2008 - 2017



COUNTERFEIT CARD FRAUD

VALUE	£24.2m	(-35%)

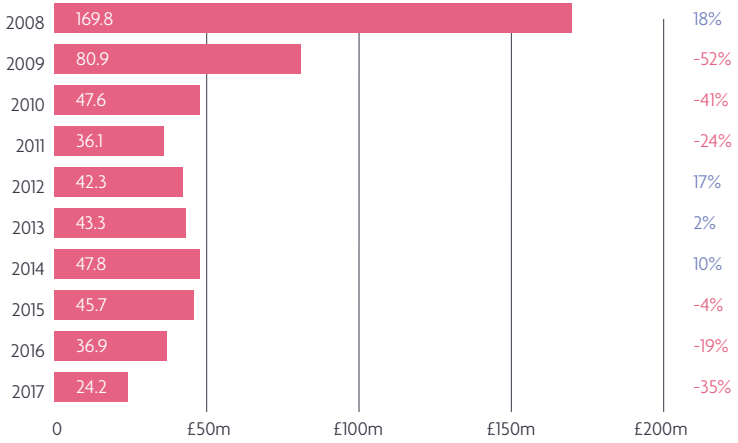
VOLUME	84,861	(-22%)

This fraud is facilitated by criminals specialising in the production of cloned cards that contain data copied from the magnetic stripe of a genuine card.

To obtain the necessary data, criminals attach concealed/disguised devices to the card-reader slots of ATMs and unattended payment terminals (UPTs), such as self-service ticket machines at railway stations, cinemas and car parks. The cloned cards are typically used overseas in countries yet to upgrade to Chip & PIN.

Counterfeit card losses totalled £24.2 million in 2017, a decrease of 35 per cent compared to 2016 and 86 per cent lower than the peak reported in 2008 (£169.8 million). The significant decreases since 2008 are likely to be a result of the introduction of chip technology in the UK and its subsequent increased adoption around the world; most notably in the United States.

Counterfeit card fraud losses on UK-issued cards 2008 – 2017



LOST AND STOLEN CARD FRAUD

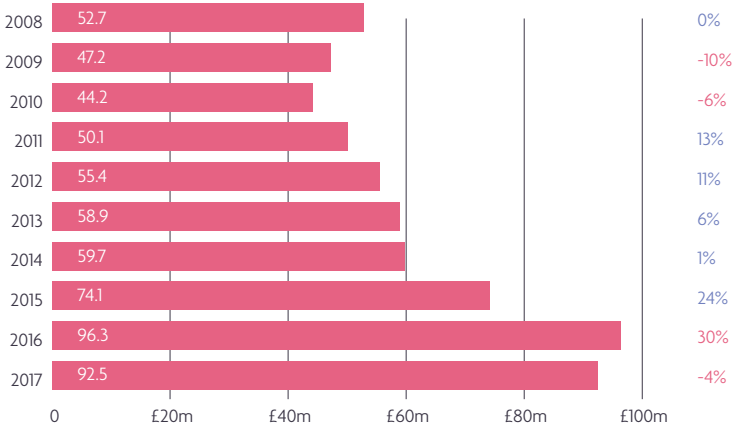
VALUE	£92.5m	(-4%)

VOLUME	350,066	(+51%)

Criminals generally rely on low-tech methods to carry out this fraud. Victims are typically shoulder-surfed for their PIN in shops and at ATMs, before falling for simple distraction tactics that enable the criminal to steal the card. In some cases, the victims are even tricked into handing their cards and PINs over to a criminal on their own doorstep, under the impression they are assisting with a police enquiry (often referred to as a courier scam).

During the year an issue was identified where a small amount of fraud was occurring on contactless cards after they had been reported lost or stolen. Technical changes have since been introduced, resulting in the majority of contactless transactions going online, meaning the transaction is authorised directly with the card issuer and an attempted purchase with a cancelled card would be declined.

Lost and stolen card fraud losses on UK-issued cards 2008 – 2017



CARD ID THEFT

VALUE	£29.9m	(-25%)

VOLUME	29,139	(-8%)

Criminals use 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
£11.3m (-28%)

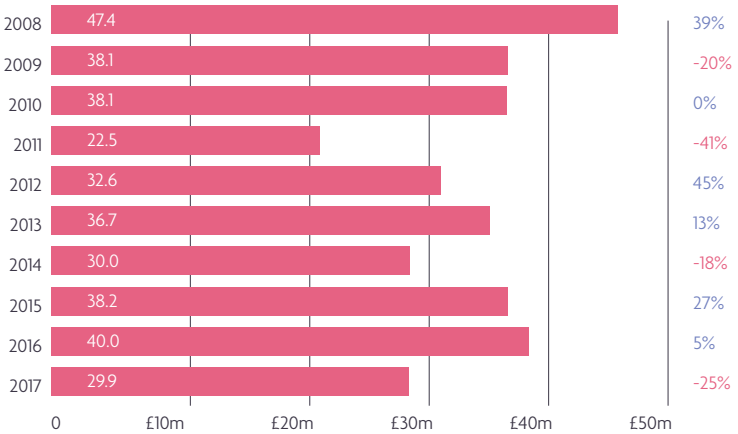
Application fraud occurs when criminals use stolen or fake documents to open an account in someone else's name. For identification purposes, criminals may try to steal documents such as utility bills and bank statements to build up useful personal information. Alternatively, they may use counterfeit documents.

Account takeover
£18.5m (-24%)

This involves a criminal fraudulently using another person's credit or debit card account, first by gathering information about the intended victim, then contacting their bank or credit card issuer to masquerade as the genuine cardholder.

The criminal then arranges for funds to be transferred out of the account or will change the address on the account and ask for new or replacement cards to be sent.

ID theft on UK-issued cards 2008 – 2017



CARD NON-RECEIPT FRAUD

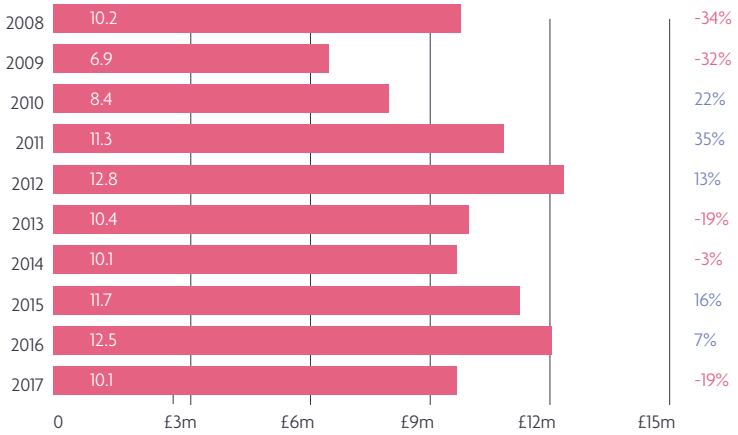
VALUE	£10.1m	(-19%)

VOLUME	10,905	(-4%)

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

Properties with communal letterboxes, such as flats and student halls of residence, and people who do not get their mail redirected when they change address are all vulnerable to this type of fraud.

Mail non-receipt fraud losses on UK-issued cards 2008-2017



PLEASE NOTE: Figures in the following sections relate to the places where the card was used fraudulently, rather than how the card or the card details were compromised. This is simply another way of breaking the overall 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, e.g. a lost or stolen card could be used to make an ATM withdrawal as well as to purchase goods on the high street.

UK RETAILER FACE-TO-FACE CARD FRAUD LOSSES

VALUE	£61.8m	(-2%)

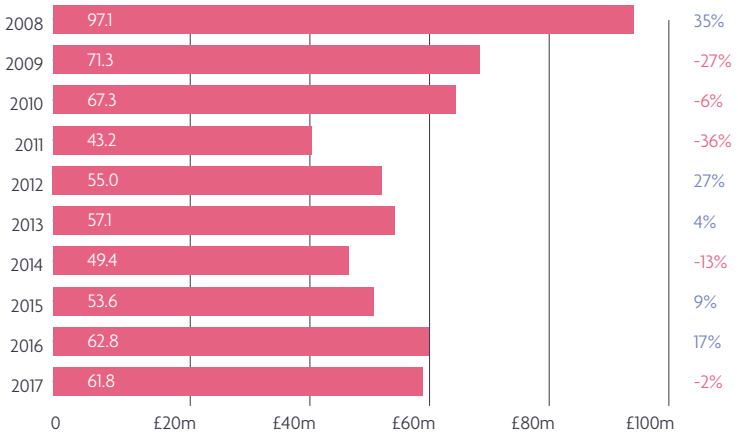
Fraud losses on face-to-face purchases on the UK high street fell two per cent in 2017 to £61.8 million.

Most of this fraud is undertaken using basic techniques, with fraudsters finding ways of stealing the card, and often the PIN, to carry out fraudulent transactions in shops and at ATMs. For example, criminals are targeting cards and PINs using techniques such as ATM card entrapment, distraction theft and shoulder surfing and various social engineering methods to dupe victims into handing over their cards on their own front door step.

This total includes fraud incidents on both contactless cards and mobile devices. Fraud on contactless cards and devices remain low with £14 million of losses during 2017, compared to spending of £52.4 billion over the same period.

This is equivalent to 2.7p of fraud losses every £100 spent using contactless technology, the same as it was in 2016. Fraud on contactless cards and devices represents just 2.5 per cent of overall card fraud losses, while 31 per cent of all card transactions were contactless last year. No contactless fraud has been recorded on cards still in the possession of the original owner.

Card fraud losses at UK retailers (face-to-face transactions) 2008-2017



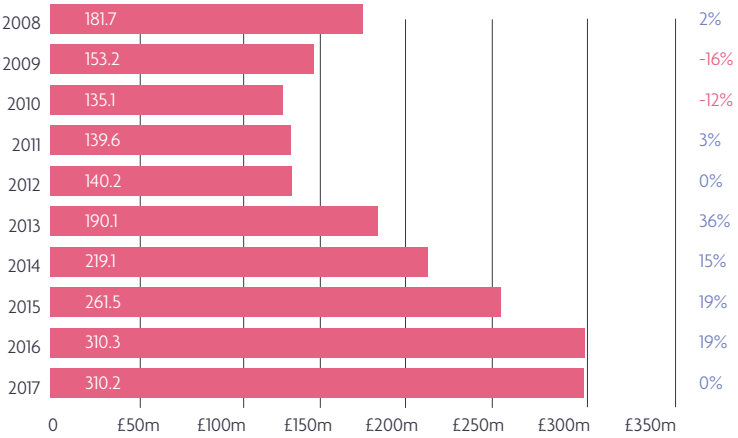
INTERNET/E-COMMERCE FRAUD

VALUE	£310.2m	(0%)

These figures are included within the overall remote purchase (card-not-present) fraud losses described in the previous section. An estimated £310.2 million of e-commerce fraud took place on cards in 2017, accounting for 55 per cent of all card fraud and 76 per cent of total remote purchase fraud.

Total e-commerce sales on sites based in the UK during 2017 was £222 billion, meaning that for every £100 spent online at UK merchants only 9.3p was fraudulent. For online merchants based overseas, 23p in every £100 spent was fraudulent.

Internet/e-commerce fraud losses on UK issued cards 2008-2017



CARD FRAUD AT UK CASH MACHINES

VALUE	£37.2m	(-14%)

These figures show how much fraud takes place at cash machines in the UK, either using 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.

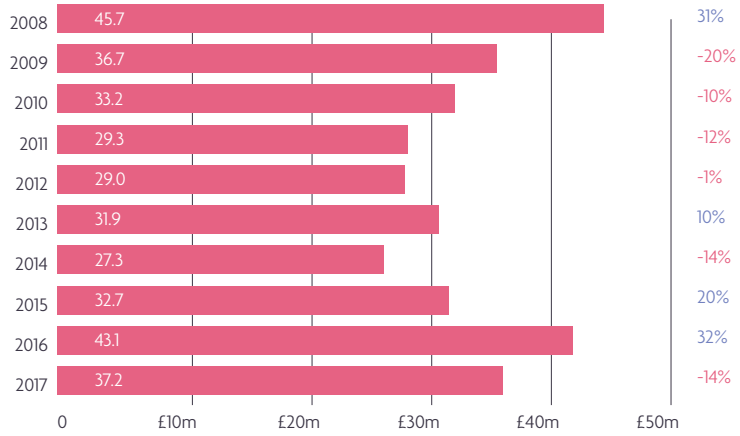
Fraudsters also target cash machines to compromise or steal cards or card details in three main ways:

Entrapment devices: Inserted into a cash machines card slot, these devices keep the card inside the machine. The criminal also captures the PIN by using a small camera attached to the machine or by watching it being entered. After the cardholder gives up and leaves, the criminal removes the device with the card and subsequently withdraws cash.

Skimming devices: These devices are attached to the cash machine to record the details from the magnetic strip of a card, while 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 pickpocketing.

Fraud losses at UK cash machines 2008-2017



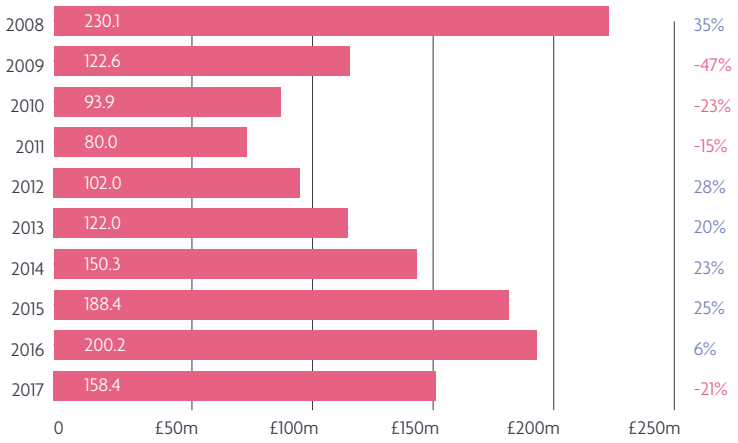
CARD FRAUD ABROAD

VALUE	£158.4m	(-21%)

The majority (79 per cent) of this type of fraud is attributed to remote purchase fraud at overseas retailers. This category also includes cases where criminals steal the magnetic stripe details from UK-issued cards, to make counterfeit cards, which are used overseas in countries yet to upgrade to Chip & PIN. This type of fraud has fallen when compared to previous years, because of the increased adoption of chip technology around the globe.

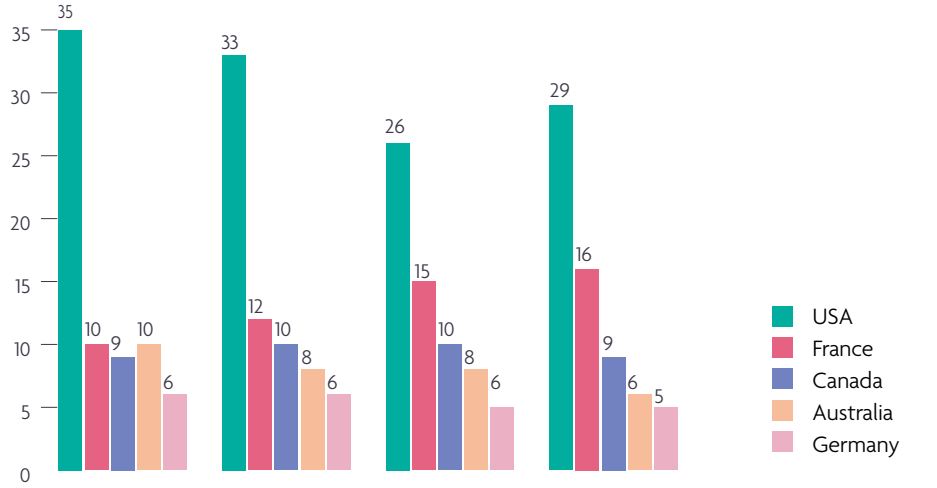
International fraud losses for 2017 were £158.4 million a decrease of 31 per cent, compared with losses at their peak in 2008 (£230.1 million).

Fraud committed abroad on UK-issued cards 2008-2017



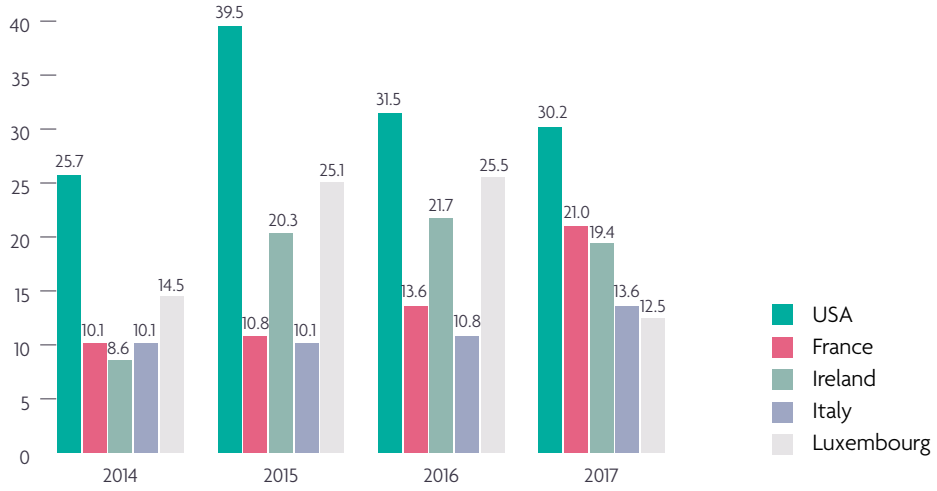
Top five countries for fraud on foreign-issued cards occurring in the UK 2014-2017

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



Top five countries where fraud on UK-issued cards occurs 2014-2017

Losses on UK-issued cards or card details used fraudulently overseas.



CHEQUE FRAUD

VALUE	£9.8m	(-28%)

VOLUME	1,745	(-48%)

Cheque fraud losses fell to £9.8 million in 2017, a 28 per cent drop on 2016, the lowest year ever reported.

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

Counterfeit cheque fraud
£2.7m -46%

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

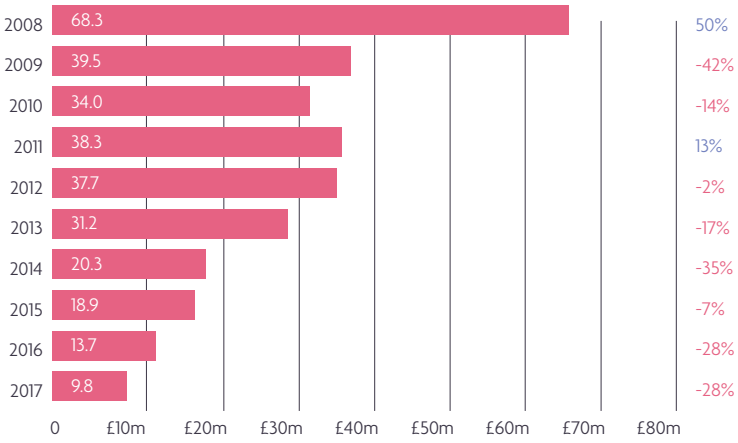
Forged cheque fraud
£4.3m -22%

A forged cheque is a genuine cheque that has been stolen from a customer and used by a fraudster with a forged signature.

Fraudulently altered cheques
£2.8m -10%

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

Cheque fraud losses 2008-2017



Annual case volumes, cheque fraud 2013-2017

YEAR	2013	2014	2015	2016	2017	% CHANGE 16/17
Cheque Fraud	10,471	8,168	5,746	3,388	1,745	-48%

ONLINE BANKING FRAUD

VALUE	£121.4m	(+19%)

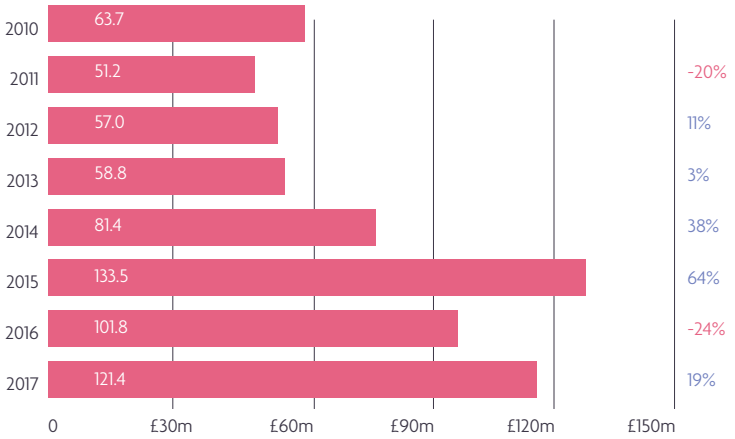
VOLUME	21,784	(+8%)

This type of fraud occurs when a fraudster gains access to a customer's online bank account and makes an unauthorised transfer of money.

Criminals often use social engineering tactics to trick customers into revealing their online banking security details, through scam phone calls, texts and emails. These details are then used to access a customer's online account and to make an unauthorised transaction.

Collection of industry fraud losses for online banking began in June 2009. Case volumes were not collected until 2012. Cases where the customer has authorised a transaction are reported separately on page 33.

Online banking fraud losses 2010-2017



Annual case volumes for online banking fraud 2012-2017

YEAR	2012	2013	2014	2015	2016	2017	% CHANGE 16/17
Online Banking Fraud	16,355	13,799	16,041	19,691	20,088	21,784	8%

PHONE BANKING FRAUD

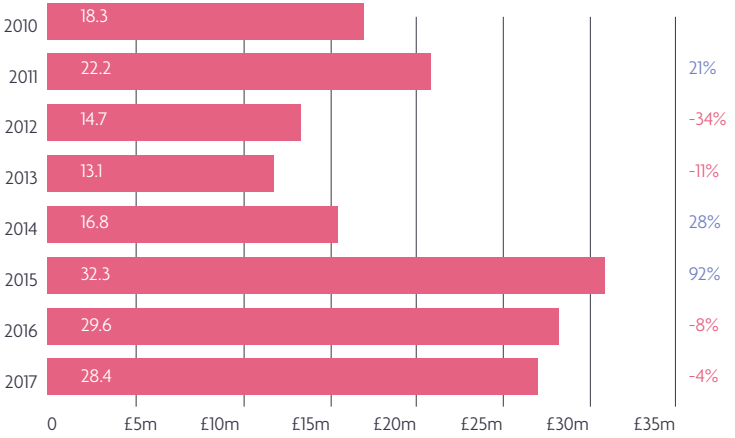
VALUE	£28.4m	(-4%)

VOLUME	9,575	(-9%)

This fraud happens when a criminal fraudulently accesses the victim's phone banking account and makes an unauthorised transfer of money from the account.

Like online banking fraud, criminals often use social engineering tactics to trick customers into revealing their account security details, which are then used to convince the telephone banking operator that they are the genuine account holder. Collection of industry fraud losses for telephone banking fraud began in June 2009. Case volumes were not collected until 2012. Cases where the customer has authorised a transaction are reported separately on page 33.

Phone banking fraud losses 2010-2017



Annual case volumes for phone banking fraud 2012-2017

YEAR	2012	2013	2014	2015	2016	2017	% CHANGE 16/17
Phone Banking Fraud	7,095	5,596	5,778	11,380	10,495	9,575	-9%

AUTHORISED PUSH PAYMENT FRAUD

VALUE	£236m	N/A

VOLUME	43,875	N/A

For the first time in 2017 UK Finance published the level of losses caused by authorised push payment (APP) scams. This fraud category differs to the rest of the statistics published in this document, as the genuine account holder is tricked into making the payment to a fraudster.

Total losses due to APP scams were £236 million in 2017, with 43,875 cases relating to a total of 42,837 victims.

In 2017, criminals' use of social engineering tactics through deception and impersonation scams continued to be a key driver of authorised fraud losses. Social engineering is a method through which criminals manipulate people into transferring money directly to the them. In an impersonation scam, fraudsters contact customers by phone, text message or email 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. Criminals use these fraudulent approaches to trick the victim into authorising a payment to them. Other common scripts include impersonating bank staff or police officials and claiming the customer's local branch is under investigation and that money needs to be transferred to a 'safe account'; sending fake invoices to businesses; offering bogus investment opportunities; and through online auction scams.

TAKE FIVE TO STOP FRAUD

Take Five to Stop Fraud is a national campaign that offers advice to help everyone protect themselves against preventable financial fraud. It is led by UK Finance and backed by government.

Take Five helps customers to confidently challenge any requests for their personal or financial information, or to transfer money to a fraudster's account. It focuses on financial frauds directly targeting customers, including email deception and phone-based scams as well as online fraud – particularly where criminals impersonate trusted organisations.

The campaign is being delivered with and through a range of partners in the UK payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector organisations.

To help everyone stay safe from fraud and scams, Take Five to Stop Fraud urges customers to follow its campaign advice.

(See next page)

HM Government

Financial Fraud Action UK
Working together to prevent fraud

STOP AND THINK

1. A genuine bank or organisation will never contact you out of the blue to ask for your PIN, full password or to move money to another account. Only give out your personal or financial details to use a service that you have given your consent to, that you trust and that you are expecting to be contacted by.

2. Don't be tricked into giving a fraudster access to your personal or financial details. Never automatically click on a link in an unexpected email or text.

3. Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.

takefive-stopfraud.org.uk

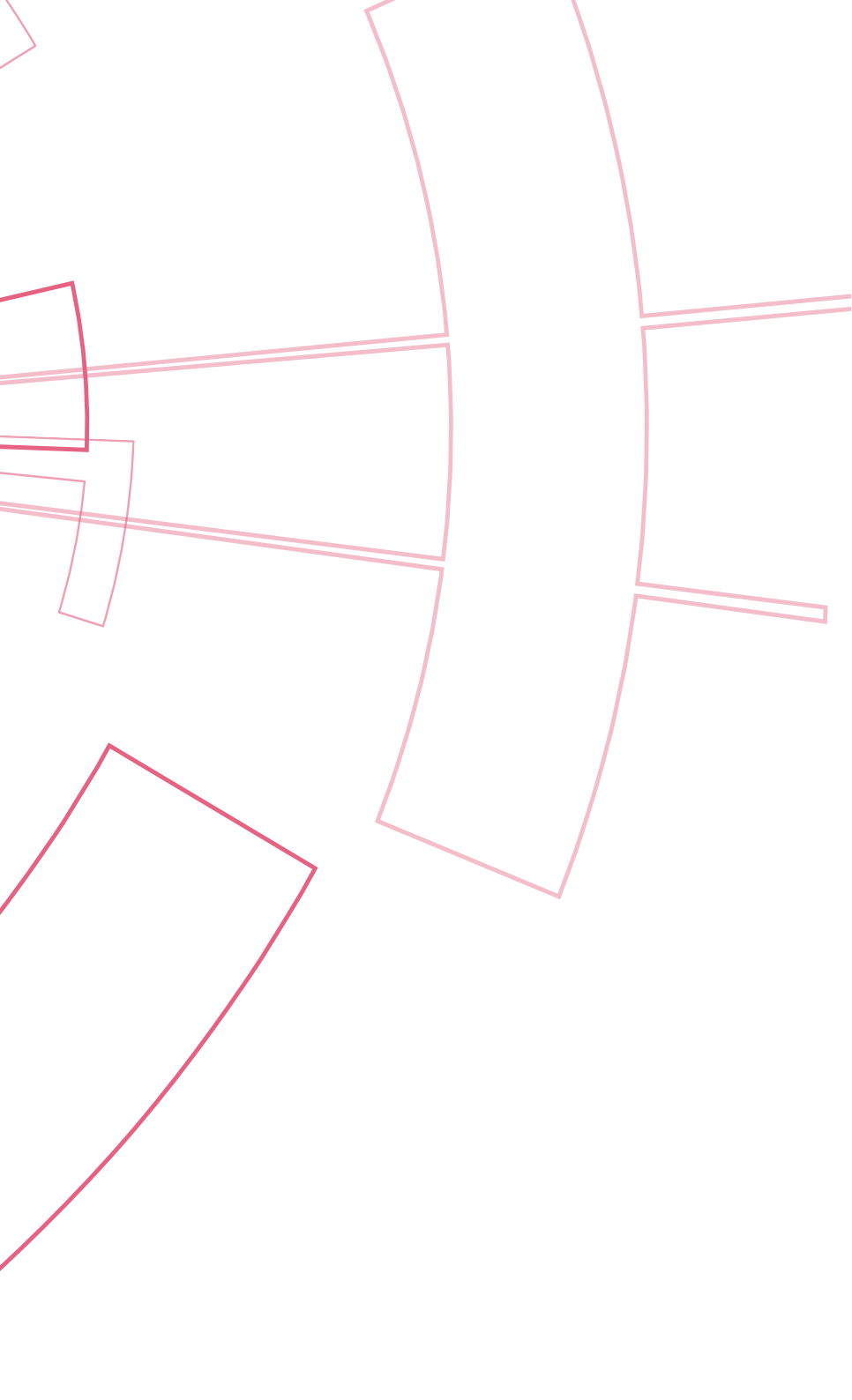
TAKE FIVE
TO STOP FRAUD™

LIST OF CONTRIBUTING MEMBERS

As of 1 January 2018

These members contributed to the statistics in this publication:

- Allied Irish Bank (UK) plc
- American Express Services Ltd
- Bank of America
- Bank of Ireland
- Barclays Bank
- Capital One (Europe) plc
- C Hoare Co
- Citibank
- The Co-operative Bank plc
- Coventry Building Society
- Danske Bank (trading name of Northern Bank Ltd)
- HSBC
- Investec Bank plc
- JPMorgan Chase and Co.
- Lloyds Banking Group Ltd
- Metro Bank plc
- Clydesdale Bank (including Yorkshire Bank)
- Nationwide
- NewDay Ltd
- Royal Bank of Scotland Group Ltd
- Sainsburys Bank plc
- Santander UK plc
- Tesco Bank plc
- Triodos
- TSB Bank plc
- Vanquis Bank
- Virgin Money
- Yorkshire Building Society



www.ukfinance.org.uk
UK Finance
1 Angel Court
London, EC2R 7HJ
United Kingdom