



Financial Fraud ActionUK  
Working together to prevent fraud

2017

# FRAUD THE FACTS 2017

THE DEFINITIVE OVERVIEW OF PAYMENT INDUSTRY FRAUD



### **FFA UK's 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.
- // 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

### **It does this by:**

- // 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, a unique proactive operational police unit with a national remit, formed as a partnership between FFA UK, the City of London Police, and the Metropolitan Police
- // Managing intelligence-sharing through the industry fraud 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
- // Informing commentators and policy-makers through our 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

## 06

Introduction

## 10

2016 overview

## 12

Card fraud

|  |    |
|--|----|
| Remote purchase fraud                      | 16 |
| Counterfeit card fraud                     | 17 |
| Lost and stolen card fraud                 | 18 |
| Card ID theft                              | 19 |
| Card non-receipt fraud                     | 21 |
| UK retailer face-to-face card fraud losses | 22 |
| Internet/e-commerce fraud                  | 24 |
| Card fraud at UK cash machines             | 26 |
| Card fraud abroad                          | 28 |

## 30

Cheque fraud

## 32

Online banking fraud

## 33

Phone banking fraud

## 34

Phishing

## 36

Combatting financial fraud

## 38

Membership list



# Introduction

**Katy Worobec**

Director, Financial Fraud Action UK

Our members take the threat of fraud extremely seriously and continuously invest in advanced detection and verification systems to protect customers, which stopped £6.40 in every £10 of attempted fraud last year.

However, we know that criminals continue to attempt to circumvent these systems by targeting customers for their personal and security information. Impersonation and deception scams, as well as digital attacks, continue to be the primary factor behind financial fraud losses.

That is why last year, Financial Fraud Action UK and its members, in collaboration with supporters in government and law enforcement, launched Take Five to Stop Fraud. The campaign seeks to put consumers and businesses back in control with straightforward advice to help prevent financial fraud.

We have also continued our collaboration through the Joint Fraud Taskforce, which was established by the then Home Secretary, Theresa May, in February 2016, to use the collective powers, systems and resources of government, law enforcement and industry to crack down on financial fraud.

FFA UK works in partnership with The UK Cards Association in developing and delivering fraud strategy on credit, debit and charge cards. UK Cards is the trade body for the card payments industry in the UK, representing financial institutions which act as card issuers and acquirers.

It also works with the Cheque and Credit Clearing Company (C&CCC), the industry body that manages the cheque clearing system in Great Britain, including the processing of bankers' drafts, building society cheques, postal orders, warrants and government payable orders.





# Trends and Statistics





# 2016 overview

Financial fraud losses across payment cards, remote banking and cheques totalled £768.8 million in 2016, an increase of 2 per cent compared to 2015.

Prevented fraud totalled £1.38 billion in 2016. This represents incidents that were detected and prevented by the banks and card companies and is equivalent to £6.40 in every £10 of attempted fraud being stopped.

## Drivers of the changing fraud figures

While it is not possible to place specific monetary values on particular modus operandi, intelligence reported into FFA UK by its members indicates the key drivers behind the reported figures.

The rise across all fraud loss types seen during 2016 owes much to the growth of impersonation and deception scams, as well as sophisticated online attacks such as malware and data breaches.

These methods all aim to compromise customers' personal and financial details, including card data, in order to enable the criminals to commit fraud.

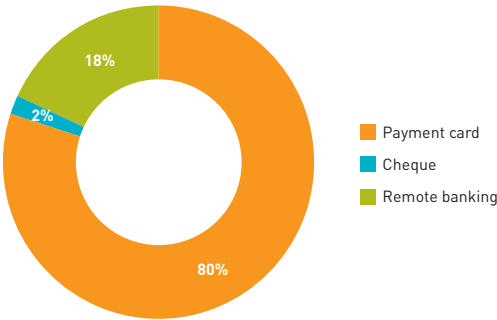
In an impersonation and deception scam, a criminal approaches a customer purporting to be a legitimate organisation. These scams typically involve a phone call, text message or email, in which the criminal claims to be from a trusted organisation such as a bank, the police, a utility company or a government department.

The fraudulent approach often claims that there has been suspicious activity on the recipient's account or that their account details need to be 'updated' or 'verified'. The criminal then attempts to trick their victim into giving away their personal or financial information, such as passwords or passcodes, or into transferring money directly to the fraudster.

There have been several high profile data breaches reported in 2016, along with more frequent lower level attacks. This data can be used to commit fraud directly, for example the use of stolen card details to make remote purchases. Other personal and financial information obtained in a breach can be used in impersonation scams, while the publicity around the incident itself can be used to add authenticity to the fraudulent approach.

Criminal gangs also use malware (malicious software which is unknowingly downloaded onto a device or computer) and phishing emails as a means to compromise customers' security and personal details. Once obtained, fraudsters will use these details to access customer accounts or to commit fraud.

TOTAL 2016 FINANCIAL FRAUD  
LOSSES BY TYPE



*The data reported here includes 3rd party fraud on all core banking products/services (including credit and charge cards, current accounts and debit cards, savings accounts, cheques, overdrafts and loans): channels (including point of sale, remote purchases, online/telephone banking, branch counter) and customers (personal and business).*

# CARD FRAUD

|       |         |     |             |           |      |
|-------|---------|-----|-------------|-----------|------|
| VALUE | £618.0m | +9% | CASE VOLUME | 1,820,726 | +22% |
|-------|---------|-----|-------------|-----------|------|

Fraud losses on UK issued cards totalled £618.0 million in 2016, a 9% increase from £567.5 million in 2015; the fifth consecutive year of increase and higher than the peak of £609.9 million seen in 2008. At the same time, total spending on all debit and credit cards reached £904 billion in 2016, with 19.1 billion transactions made during the year.

Overall card fraud losses as a proportion of the amount we spend on our cards has decreased slightly during 2016, falling from 8.4p per £100 spent in 2015 to 8.3p per £100 in 2016 (in 2008 it was 12.4p for every £100 spent). This indicates that although payment card fraud is increasing, it is doing so at a slightly slower rate than genuine usage.

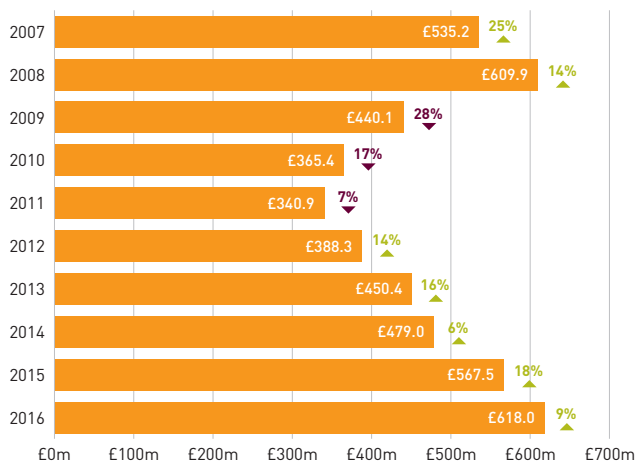
These trends owe much to the use of deception crimes, as well as the use of online attacks, such as malware and data hacks, to compromise card details. In response, the industry has redoubled its efforts to warn consumers and online businesses to install security software which is often available for 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 (such as American Express 'SafeKey', Mastercard 'SecureCode' and 'Verified by Visa').

## Fraud volumes

FFA UK also publishes 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 2016 figures showing a significant increase in comparison to 2015 particularly in the remote purchase (CNP) and lost & stolen categories.

## FRAUD LOSSES ON UK-ISSUED CARDS 2007–2016 (GROSS)

Arrows show percentage change on previous year's total



## ANNUAL FRAUD LOSSES ON UK-ISSUED CARDS 2007–2016

All figures in £ millions

| FRAUD TYPE                 | 2007         | 2008         | 2009         | 2010         | 2011         | 2012         | 2013         | 2014         | 2015         | 2016         | % Change 15/16 |
|----------------------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|----------------|
| Remote Purchase (CNP)      | 290.5        | 328.4        | 266.4        | 226.9        | 220.9        | 246.0        | 301.0        | 331.5        | 398.2        | 432.3        | 9%             |
| <i>Of which e-commerce</i> | 178.3        | 181.7        | 153.2        | 135.1        | 139.6        | 140.2        | 190.1        | 219.1        | 261.5        | 308.8        | 18%            |
| Counterfeit                | 144.3        | 169.8        | 80.9         | 47.6         | 36.1         | 42.1         | 43.4         | 47.8         | 45.3         | 36.9         | -19%           |
| Lost & Stolen              | 56.2         | 54.1         | 47.7         | 44.4         | 50.1         | 55.2         | 58.9         | 59.7         | 74.1         | 96.3         | 30%            |
| Card ID Theft              | 34.1         | 47.4         | 38.2         | 38.1         | 22.5         | 32.2         | 36.7         | 29.9         | 38.2         | 40.0         | 5%             |
| Card non-receipt           | 10.2         | 10.2         | 6.9          | 8.4          | 11.3         | 12.8         | 10.4         | 10.1         | 11.7         | 12.5         | 7%             |
| <b>TOTAL</b>               | <b>535.2</b> | <b>609.9</b> | <b>440.1</b> | <b>365.4</b> | <b>340.9</b> | <b>388.3</b> | <b>450.4</b> | <b>479.0</b> | <b>567.5</b> | <b>618.0</b> | <b>9%</b>      |
| UK                         | 327.6        | 379.7        | 317.5        | 271.5        | 260.9        | 286.7        | 328.4        | 328.7        | 379.8        | 418.0        | 10%            |
| Fraud Abroad               | 207.6        | 230.1        | 122.6        | 93.9         | 80.0         | 101.6        | 122.0        | 150.3        | 187.7        | 200.1        | 7%             |

Due to the rounding of figures, the sum of separate items may differ from the totals shown.

E-commerce figures are estimated.

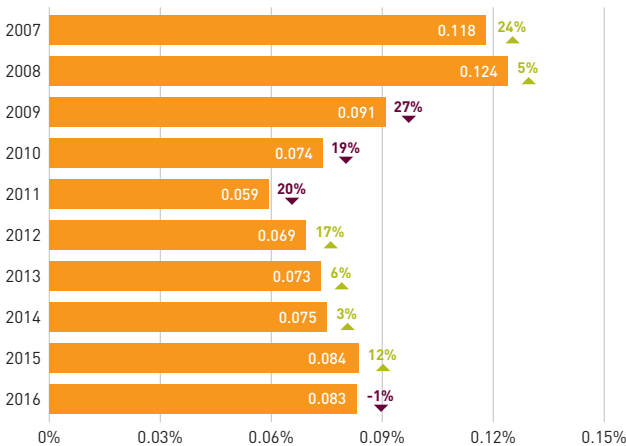
## ANNUAL CASE VOLUMES ON UK-ISSUED CARDS 2012–2016

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

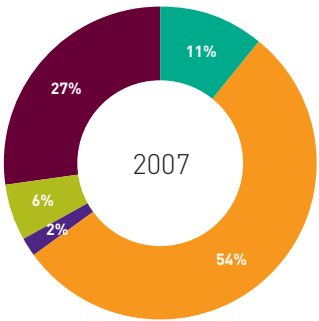
| CARD FRAUD TYPE ON UK-ISSUED CREDIT AND DEBIT CARDS | 2012           | 2013             | 2014             | 2015             | 2016             | % Change 15/16 |
|---|----------------|------------------|------------------|------------------|------------------|----------------|
| Remote Purchase (CNP)                               | 750,200        | 951,998          | 1,019,146        | 1,194,482        | 1,437,832        | 20%            |
| Counterfeit (skimmed/cloned)                        | 98,322         | 101,109          | 99,279           | 92,670           | 108,597          | 17%            |
| Fraud on lost or stolen cards                       | 113,003        | 138,967          | 133,943          | 152,727          | 231,164          | 51%            |
| Card ID theft                                       | 24,078         | 30,718           | 26,542           | 36,318           | 31,756           | -13%           |
| Card non-receipt                                    | 9,018          | 9,125            | 9,302            | 10,914           | 11,377           | 4%             |
| <b>TOTAL</b>  | <b>994,621</b> | <b>1,231,917</b> | <b>1,288,662</b> | <b>1,487,111</b> | <b>1,820,726</b> | <b>22%</b>     |

## FRAUD TURNOVER RATIO 2007–2016

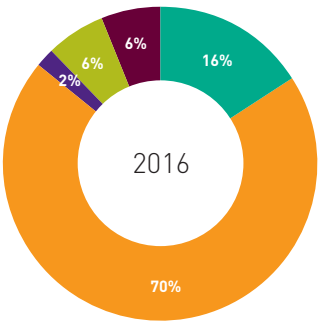
Arrows show percentage change on previous year's total



CARD FRAUD LOSSES SPLIT BY TYPE  
As percentage of total losses



- Lost / stolen card
- Remote purchase
- Card not received
- ID theft
- Counterfeit card



- Lost / stolen card
- Remote purchase
- Card not received
- ID theft
- Counterfeit card

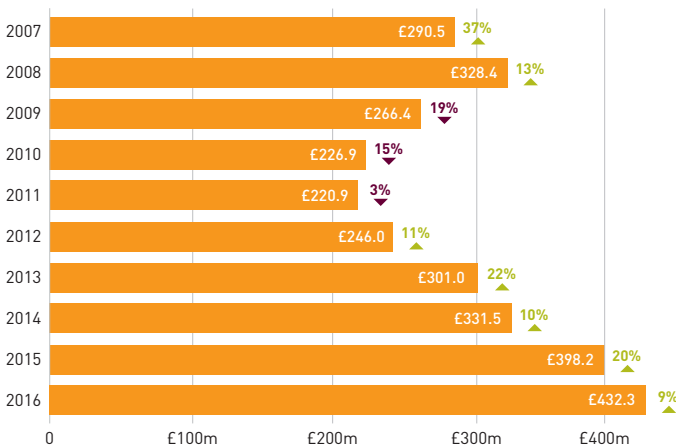


# Remote purchase fraud (internet, telephone, mail order)

|             |           |      |
|-------------|-----------|------|
| VALUE       | £432.3m   | +9%  |
| CASE VOLUME | 1,437,832 | +20% |

## REMOTE PURCHASE (CNP) FRAUD LOSSES ON UK-ISSUED CARDS 2007–2016

Arrows show percentage change on previous year's total



The vast 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 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.

Online fraud against UK retailers totalled an estimated £189.4 million in 2016, a rise of 20% on the previous year. There was also a substantial rise in fraud against online retailers based abroad, rising 15% to £119.4 million.

# Counterfeit card fraud

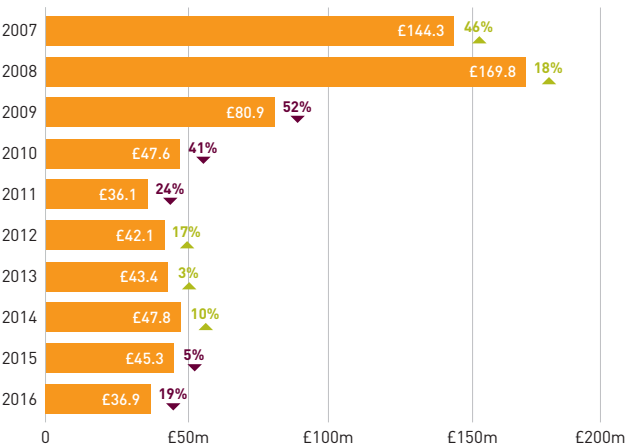
|             |         |      |
|-------------|---------|------|
| VALUE       | £36.9m  | -19% |
| CASE VOLUME | 108,597 | +17% |

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 adopt chip cards.

## COUNTERFEIT CARD FRAUD LOSSES ON UK-ISSUED CARDS 2007–2016

Arrows show percentage change on previous year's total



# Lost and stolen card fraud

|             |         |      |
|-------------|---------|------|
| VALUE       | £96.3m  | +30% |
| CASE VOLUME | 231,164 | +51% |

This category covers fraud on cards that have been reported by the cardholder as lost or stolen.

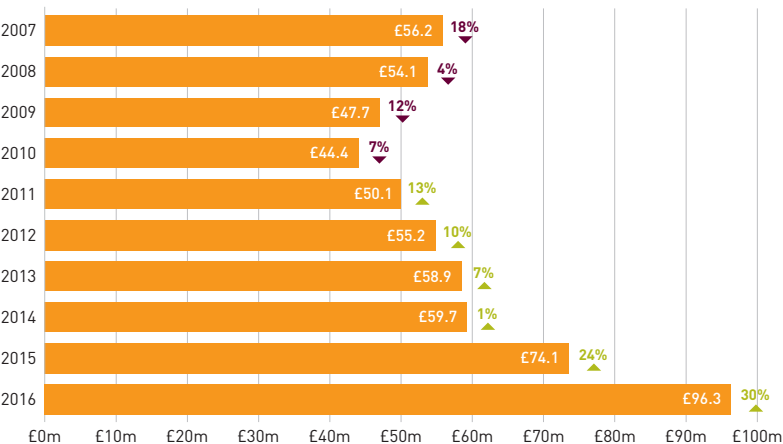
Lost and stolen cards can be used in shops that do not have Chip & PIN, or to commit a fraudulent telephone, internet or mail order transaction. If the PIN is also obtained, the card could be used in a shop or cash machine.

Initiatives such as Chip & PIN have made it harder to commit frauds using a card without having the PIN. Fraudsters are instead focused on frauds that enable them to steal both people’s cards and PINs. These 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 door step (often referred to as courier scams or telephone scams).

An issue was identified where a small amount of fraud was occurring on contactless cards that had been reported lost or stolen. Following the identification of this issue, industry has moved to change procedures and where necessary, develop improvements. All changes will be made by the end of June 2017.

## LOST AND STOLEN FRAUD LOSSES ON UK-ISSUED CARDS 2007–2016

Arrows show percentage change on previous year’s total



# Card ID theft

|             |        |      |
|-------------|--------|------|
| VALUE       | £40.0m | +5%  |
| CASE VOLUME | 31,756 | -13% |

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

£15.6m  11%

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

## ACCOUNT TAKEOVER

£24.4m  1%

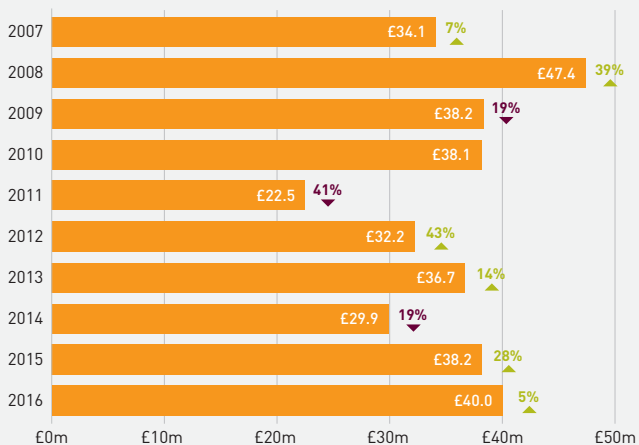
This involves a criminal fraudulently using another person's credit or debit card account, first by gathering information about the intended victim, then contacting their bank or credit card issuer to masquerade as the genuine cardholder.

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 2007–2016

Arrows show percentage change on previous year's total



# Card non-receipt fraud

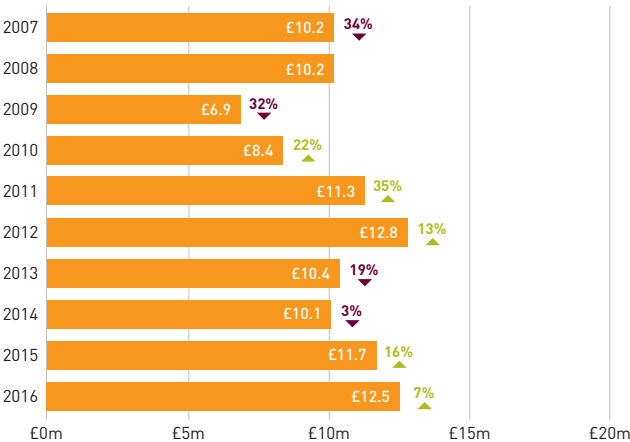
|       |        |     |             |        |     |
|-------|--------|-----|-------------|--------|-----|
| VALUE | £12.5m | +7% | CASE VOLUME | 11,377 | +4% |
|-------|--------|-----|-------------|--------|-----|

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.

## MAIL NON-RECEIPT FRAUD LOSSES ON UK-ISSUED CARDS 2007–2016

Arrows show percentage change on previous year's total



**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.*

## UK retailer face-to-face card fraud losses

|       |        |      |
|-------|--------|------|
| VALUE | £62.8m | +17% |
|-------|--------|------|

Fraud losses on face to face purchases on the UK high street increased by 17% in 2016 to £62.8 million. However, losses are still 71% lower than the peak of £218.8 million in 2004, prior to the roll out of Chip & PIN in the UK.

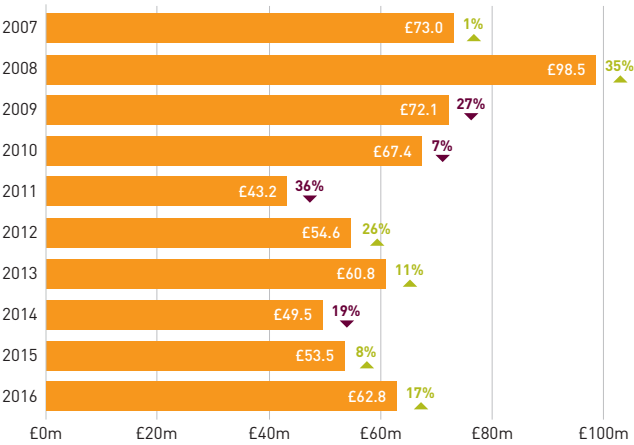
The majority of this fraud is undertaken using more basic techniques, with fraudsters finding ways of stealing both the card and PIN in order to carry out fraudulent transactions in shops and stores. For example, criminals are targeting cards and PINs through distraction theft and shoulder surfing, as 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 use compromised cards in the UK.

These totals include fraud incidents on both contactless cards and mobile devices. Fraud on contactless cards and devices remains low with £6.9 million of losses during 2016, compared to spending of £25.2 billion over the same period. This is equivalent to 2.7p in every £100 spent using contactless technology while fraud on contactless cards and devices accounts for only 1 per cent of overall card fraud.



CARD FRAUD LOSSES AT UK RETAILERS  
(FACE-TO-FACE TRANSACTIONS) 2007–2016

Arrows show percentage change on previous year's total



# Internet/e-commerce fraud

VALUE    **£308.8m**    **+18%**

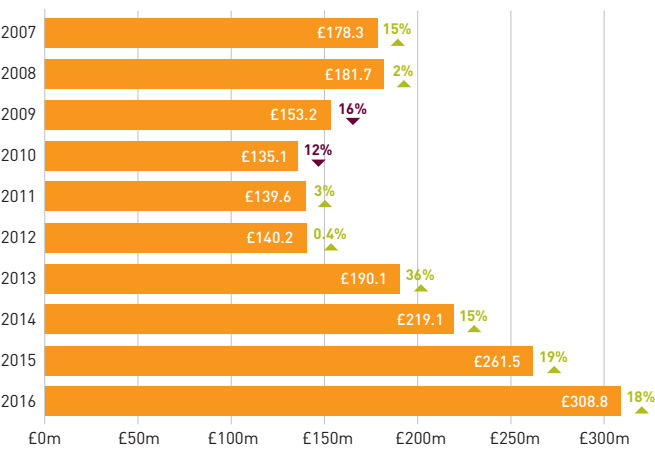
These figures are included within the overall remote purchase (CNP) fraud losses described in the previous section. An estimated £308.8 million of e-commerce fraud took place on cards in 2016, accounting for 50% of all card fraud and 71% of total remote purchase fraud.

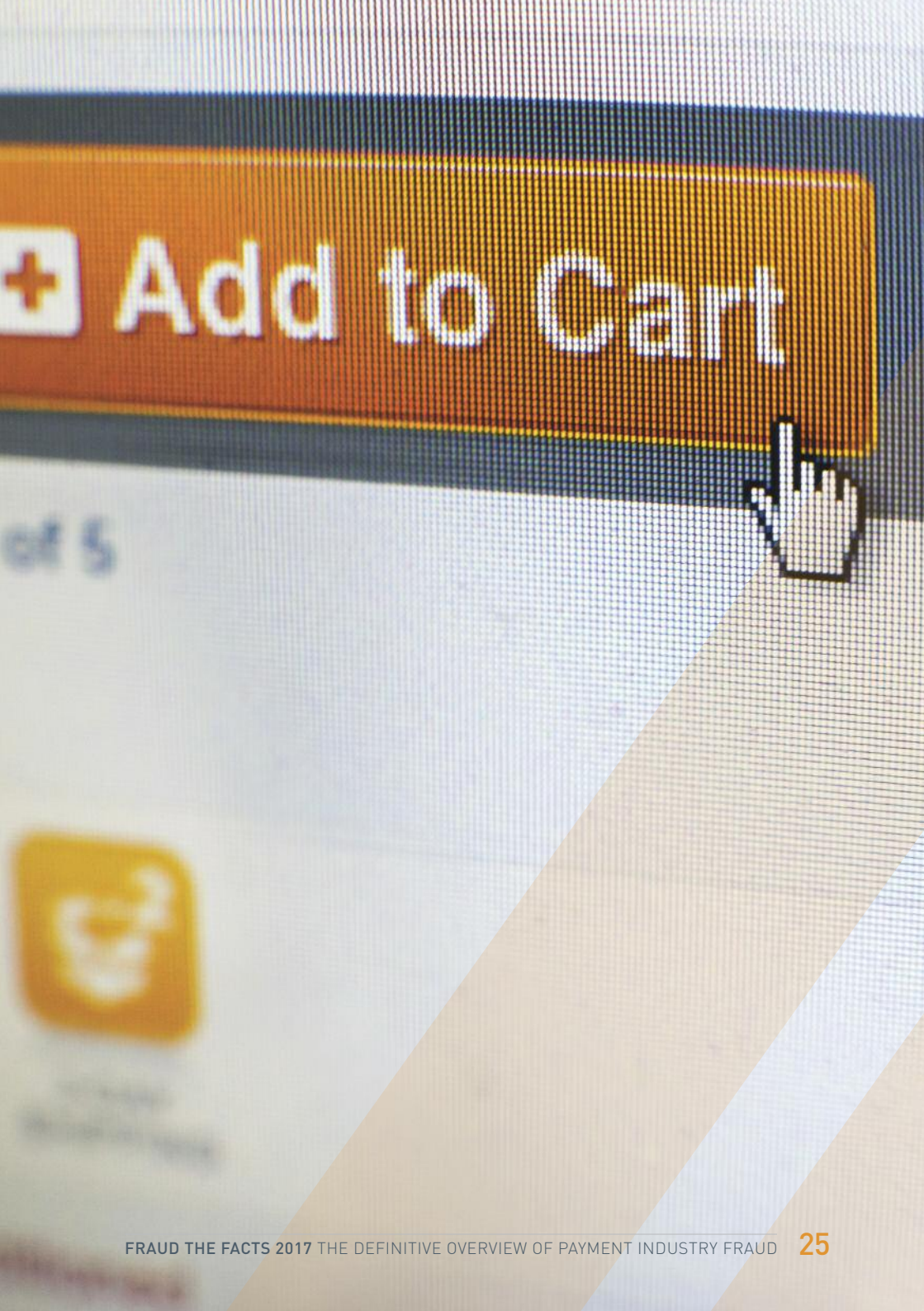
While e-commerce fraud has reached its highest point since data collection began in this area, this is to be anticipated given the considerable increase in genuine usage in this channel over the last 10 years.

Total e-commerce sales in the UK in 2016 were £199 billion, meaning that for every £100 spent online at UK merchants only 9.5 pence was fraudulent. For online merchants based overseas, 24.3 pence for every £100 was fraudulent.

## INTERNET/E-COMMERCE FRAUD LOSSES ON UK-ISSUED CARDS 2007–2016

Arrows show percentage change on previous year's total





 Add to Cart

# Card fraud at UK cash machines

VALUE

£43.1m

+32%

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:

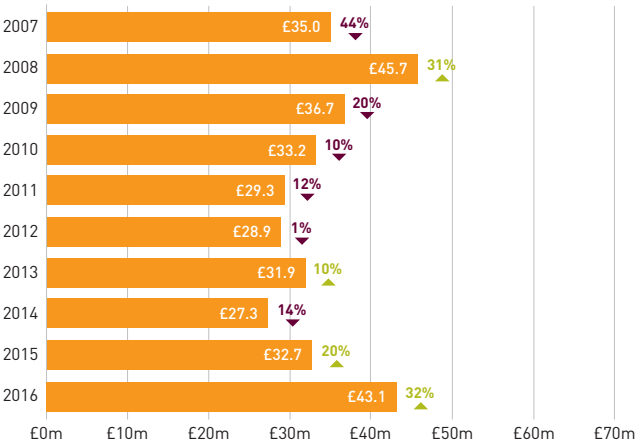
**Entrapment devices:** Inserted into a cash machine's card slot, these devices retain the card inside the machine. The criminal tricks the victim into re-entering their PIN while the criminal watches. After the cardholder gives up and leaves, the criminal removes the device with the card and subsequently 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 2007-2016

Arrows show percentage change on previous year's total



# Card fraud abroad

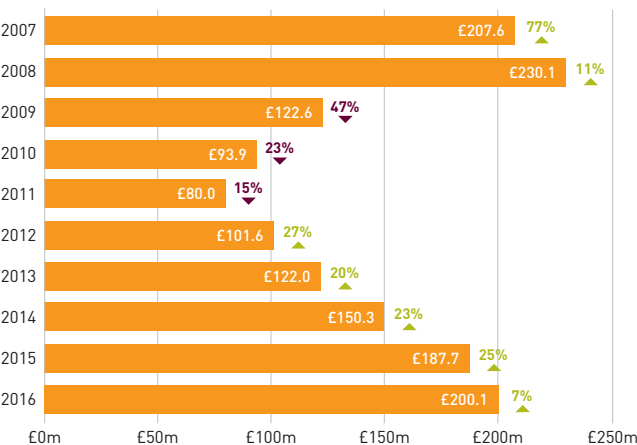
VALUE    £200.1m    +7%

The majority (74%) of this type of fraud is attributed to remote purchase fraud at retailers based overseas. This category also includes those cases where criminals steal magnetic stripe details from UK cards to make counterfeit cards for use overseas in countries yet to upgrade to Chip & PIN. However, this type of fraud has fallen when compared to previous years as a result of the increased adoption of chip technology around the globe.

International fraud losses for 2016 were £200.1 million, compared with losses at their peak in 2008 (£230.1m), a decrease of 13%.

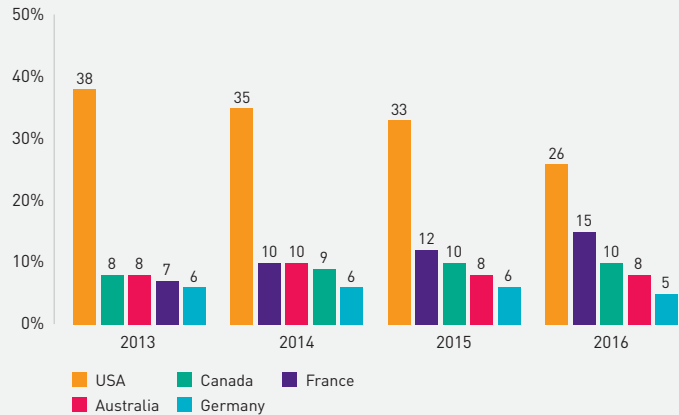
## FRAUD COMMITTED ABROAD ON UK-ISSUED CARDS 2007-2016

Arrows show percentage change on previous year's total



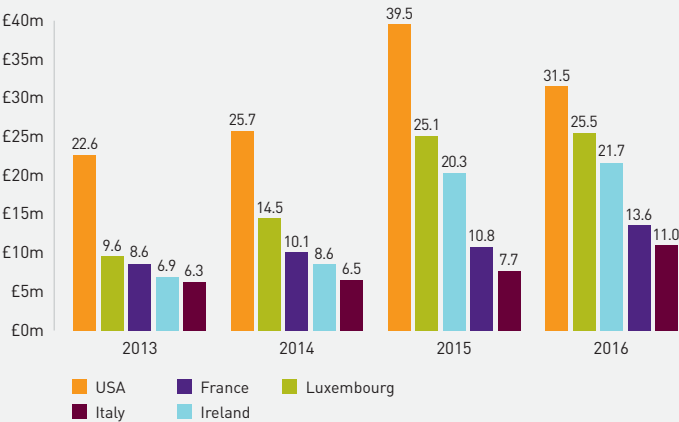
### TOP FIVE COUNTRIES FOR FRAUD ACQUIRED IN THE UK ON FOREIGN-ISSUED CARDS

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



### TOP FIVE COUNTRIES FOR FRAUD ABROAD 2013–2016

UK issued cards or card details used fraudulently overseas





# CHEQUE FRAUD

VALUE

£13.7m

-28%

CASE VOLUME

3,388

-41%

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

## Counterfeit cheque fraud

£5.0m <sup>41%</sup>▼

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

£5.5m <sup>0%</sup>

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

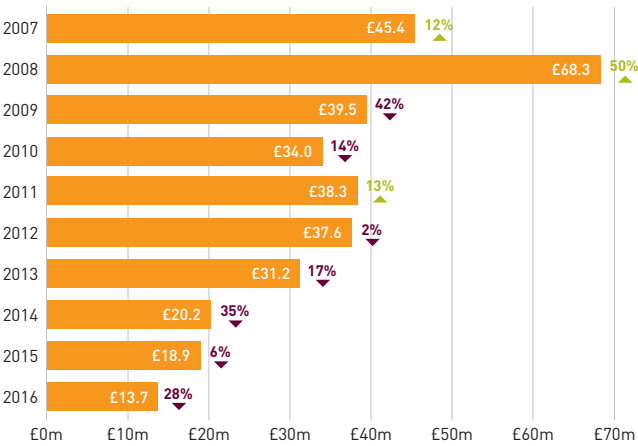
## Fraudulently altered cheques

£3.2m <sup>35%</sup>▼

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

### CHEQUE FRAUD LOSSES 2007–2016

Arrows show percentage change on previous year's total



### ANNUAL CASE VOLUMES CHEQUE FRAUD 2012–2016

|              | 2012   | 2013   | 2014  | 2015  | 2016  | % Change 15/16 |
|--------------|--------|--------|-------|-------|-------|----------------|
| CHEQUE FRAUD | 15,539 | 10,471 | 8,168 | 5,746 | 3,388 | -41%           |

# ONLINE BANKING FRAUD

|             |         |      |
|-------------|---------|------|
| VALUE       | £101.8m | -24% |
| CASE VOLUME | 20,088  | +2%  |

Online banking fraud occurs when the fraudster gains access to and transfers funds from an individual's online bank account.

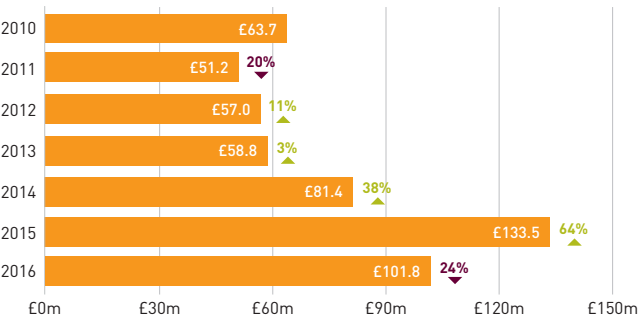
In some cases, an individual may be duped by a criminal into making a fraudulent money transfer themselves.

A range of factors are believed to have contributed to the decrease in online banking fraud, including further investment in fraud detection and prevention by the banks and also better intelligence sharing by industry and with law enforcement.

Collection of industry fraud losses for online banking fraud began in June 2009. Case volumes were not collected until 2012.

## ONLINE BANKING FRAUD LOSSES 2010–2016

Arrows show percentage change on previous year's total



## ANNUAL CASE VOLUMES ONLINE BANKING FRAUD 2012–2016

|                      | 2012   | 2013   | 2014   | 2015   | 2016   | % Change 15/16 |
|----------------------|--------|--------|--------|--------|--------|----------------|
| ONLINE BANKING FRAUD | 16,355 | 13,799 | 16,041 | 19,691 | 20,088 | +2%            |

# PHONE BANKING FRAUD

VALUE

£29.6m

-8%

CASE VOLUME

10,495

-8%

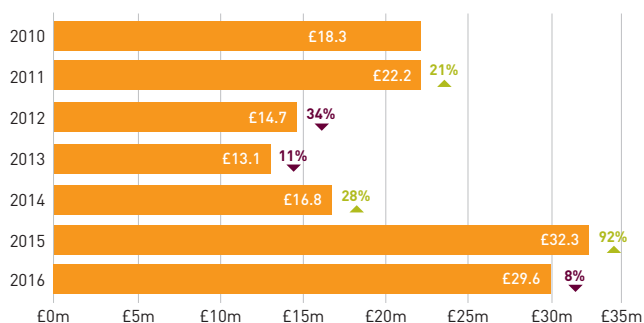
This fraud happens when a criminal fraudulently accesses the victim's phone banking account.

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, and vishing.

Collection of industry fraud losses for telephone banking fraud began in June 2009. Case volumes were not collected until 2012.

## PHONE BANKING FRAUD LOSSES 2010–2016

Arrows show percentage change on previous year's total



## ANNUAL CASE VOLUMES FOR TELEPHONE BANKING FRAUD 2012–2016

|                         | 2012  | 2013  | 2014  | 2015   | 2016   | % Change 15/16 |
|-------------------------|-------|-------|-------|--------|--------|----------------|
| TELEPHONE BANKING FRAUD | 7,095 | 5,596 | 5,778 | 11,380 | 10,495 | -8%            |



# Phishing

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 a 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 2007–2016

| 2007   | 2008   | 2009   | 2010   | 2011    | 2012    | 2013   | 2014   | 2015   | 2016   |
|--------|--------|--------|--------|---------|---------|--------|--------|--------|--------|
| 25,797 | 43,991 | 51,161 | 61,873 | 111,286 | 256,641 | 26,995 | 23,729 | 16,462 | 14,673 |

# IT PAYS TO STOP AND THINK

- 1 Never disclose security details
- 2 Don't assume an email, text or phone call is genuine
- 3 Don't be rushed
- 4 Listen to your instincts
- 5 Stay in control



**TO STOP FRAUD™**

Combating  
Financial Fraud



FFA UK delivers programmes of collaborative fraud prevention activity which combine education and awareness, intelligence-sharing and law enforcement. This work is driven by the Industry Strategic Threat Management process making it responsive to the changing patterns in fraud in the market.

This integrated approach is designed to prevent avoidable fraud, to effectively identify patterns where fraud has been committed, and to support law enforcement in bringing the criminals to justice following an attack. To ensure a coordinated response to threats, we provide expert fraud prevention advice on new initiatives pioneered by the financial services industry – for example on account switching and mobile payments. We also engage stakeholders, including regulators and government, to ensure that regulation works in step with fraud prevention programmes.

Take Five, a national fraud awareness and behaviour change campaign spearheaded by FFA UK, launched in September 2016. The campaign aims to put consumers and businesses back in control with straightforward advice to help prevent financial fraud.

It focuses on those financial frauds directly targeting customers, such as email deception (known as phishing) and phone and text-based scams (sometimes known as vishing and smishing), and is designed to remind people that it pays to stop and think.

**More information is available in the FFA UK Annual Review 2017 and on the website at:**

[www.financialfraudaction.org.uk](http://www.financialfraudaction.org.uk)

**Take Five can be found at:**

[www.takefive-stopfraud.org.uk](http://www.takefive-stopfraud.org.uk)



# List of Members

as at 1 January 2017

- // Allied Irish Bank (UK) plc
- // American Express Services Ltd
- // Bank of America
- // Bank of Ireland
- // Barclays Bank
- // Capital One (Europe) plc
- // C Hoare and Co
- // Citibank
- // The Co-operative Bank plc
- // Coventry Building Society
- // Danske Bank (*trading name of Northern Bank Ltd*)



- // Elavon Financial Services
- // First Data Europe Ltd
- // Global Payments
- // 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
- // Sainsbury's Bank plc
- // Santander UK plc
- // Tesco Bank plc
- // Triodos
- // TSB Bank plc
- // Valitor hf
- // Vanquis Bank
- // Virgin Money
- // Yorkshire Building Society

Financial Fraud Action UK

2 Thomas More Square, London E1W 1YN

[www.financialfraudaction.org.uk](http://www.financialfraudaction.org.uk)



Financial Fraud Action UK



@FFA UK

---

This document is provided for information purposes only. While every effort is made to ensure the accuracy of any information or other materials contained in this document, it is provided on the basis that Financial Fraud Action UK Ltd (and its members, 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 2017. A company registered in England No. 9529683. Published by Financial Fraud Action UK Ltd.