Financial Fraud Action UK
Working together to prevent fraud

Year-end 2016 fraud update: Payment cards, remote banking and cheque

30 March 2017

1. Introduction

Financial Fraud Action UK (FFA UK) is responsible for leading the collective fight against fraud in the UK payments industry. Its membership includes the major banks, credit, debit and charge card issuers, and card payment acquirers.

FFA UK publishes the full fraud statistics reported by its members twice yearly. The data covers payment card, remote banking and cheque fraud losses.

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

1.1. Full year fraud losses 2016

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. There were a total of 1,857,506 cases of financial fraud.

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

The proportion of prevented fraud has reduced from £7.01 in every £10 in 2015, largely due to criminals shifting their methods away from using malware attacks on online banking systems, which bank security processes identified and stopped, and towards methods less susceptible to direct bank intervention, such as scams directly targeting the customer.

1.2. Factors behind the fraud figures

It is not possible to place specific financial values on particular methods of attack, however intelligence reported to FFA UK by its members points to the key drivers behind the figures.

During 2016, criminals' use of impersonation and deception scams, as well as as well as online attacks to compromise data, continued to be the primary factor behind fraud losses. In all of these methods, criminals target personal and financial details, including card data, which are used to facilitate fraud.

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

The fraudulent approach may claim 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 the target into giving away their personal or financial information, such as passwords, payment card details or bank account information.

Intelligence suggests that criminals have recently increased their focus on phishing emails purporting to be from major online retailers and internet companies, brands which a large proportion of recipients are likely to use. These emails are increasingly sophisticated and attempt to trick recipients into giving away personal or financial details, or into downloading malware.

Information gained from data breaches also continues to be a driver of fraud. This data may be used to commit fraud directly, for example the use of stolen card details to make remote 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.

During the year, there was also intelligence reported to FFA UK of an increase in 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.

1.3. Financial fraud data

FFA UK publishes both the value of fraud losses and the volume of cases.

When looking at the data, it is important to note that each incident of fraud does not equate to one person being defrauded, but rather refers to the number of accounts that have been 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.

2. Payment card fraud

This section relates to fraud on debit, credit, charge and ATM-only cards.

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

2.1. Total UK-issued payment card fraud

Total UK-issued payment card fraud	2011	2012	2013	2014	2015	2016	% Change 15/16
Total prevented value	n/a	n/a	n/a	n/a	£843.6m	£982.4m	+16%
Total loss value	£340.9m	£388.3m	£450.4m	£479.0m	£567.5m	£618.0m	+9%
Total case volume	918,937	994,621	1,231,917	1,288,212	1,487,111	1,820,726	+22%

Fraud losses on UK-issued cards totalled £618.0 million in 2016, an increase of 9 per cent on 2015.

Over this period, overall card spending grew by six per cent. Card fraud as a proportion of card purchases therefore equates to 8.3p for every £100 spent, down from 8.4p at the end of 2015.

A total of £982.4 million of card fraud was stopped by banks and card companies in 2016, a rise of 16 per cent on 2015. This is equivalent to £6.10 in every £10 of attempted fraud being prevented before a loss occurs.

2.2. Remote purchase fraud

This type of fraud occurs when stolen payment card details are fraudulently used to make a purchase on the internet, over the telephone or through mail order. It is also referred to as card-not-present (CNP) fraud.

Remote purchase fraud	2011	2012	2013	2014	2015	2016	% Change 15/16
Total loss value	£220.9m	£246.0m	£301.0m	£331.5m	£398.2m	£432.3m	+9%
Total case volume	709,402	750,200	951,998	1,019,146	1,194,482	1,437,832	+20%

Losses on purchases made remotely increased by 9 per cent to £432.3 million in 2016.

Intelligence suggests that much of the increase is due to the use of card details stolen through data hacks and via phishing emails and smishing text messages in which fraudsters impersonate trusted brands such as online retailers.

Contained within these figures, e-commerce card fraud totalled an estimated £308.8 million, up 18 per cent compared to 2015. At the same time, online card spending increased by 18 per cent to £248 billion in 2016, up from £210 billion in 2015.

Remote purchase fraud: E-commerce / Mail order and telephone order	2011	2012	2013	2014	2015	2016	% Change 15/16
E-commerce	£139.6m	£140.2m	£190.1m	£219.1m	£261.5m	£308.8m	+18%
Mail order and telephone order (MOTO)	£81.4m	£105.6m	£111.0m	£112.4m	£136.7m	£123.5m	-10%

2.3. Lost and stolen fraud

This type of fraud occurs when a criminal uses a lost or stolen card to make a purchase (whether remotely or face-to-face) or to withdraw funds from an ATM.

Lost and stolen fraud	2011	2012	2013	2014	2015	2016	% Change 15/16
Loss value	£50.1m	£55.2m	£58.9m	£59.7m	£74.1m	£96.3m	+30%
Case volume	104,467	113,003	138,967	133,943	152,727	231,164	+51%

Lost and stolen fraud losses increased by 30 per cent in 2016 to reach £96.3 million. The number of incidents increased by 51 per cent, indicating a lower loss value per individual case.

Intelligence suggests that the increase in lost and stolen fraud is largely due to a rise in 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.

2.4. Card not received fraud

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	2011	2012	2013	2014	2015	2016	% Change 15/16
Loss value	£11.3m	£12.8m	£10.4m	£10.1m	£11.7m	£12.5m	+7%
Case volume	8,536	9,018	9,125	9,302	10,914	11,377	+4%

Card not received fraud losses increased by 7 per cent in 2016 to £12.5 million.

2.5. Counterfeit card fraud

This type of 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 as a result of criminals stealing details from a UK-issued card which is then used to make a fake magnetic stripe card for use overseas in countries yet to upgrade to Chip & PIN.

Counterfeit card fraud	2011	2012	2013	2014	2015	2016	% Change 15/16
Loss value	£36.1m	£42.1m	£43.4m	£47.8m	£45.3m	£36.9m	-19%
Case volume	81,112	98,322	101,109	99,729	92,670	108,597	+17%

Counterfeit card fraud losses fell by 19 per cent to £36.9 million in 2015. This decrease is likely due to the increased rollout of Chip technology around the world.

2.6. Card ID theft

This type of fraud 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.

Third-party application fraud occurs 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. First the criminal will gather information about the intended victim, often through deception scams, before contacting the bank or card issuer masquerading as the genuine cardholder.

Card ID theft	2011	2012	2013	2014	2015	2016	% Change 15/16
Loss value	£22.5m	£32.2m	£36.7m	£29.9m	£38.2m	£40.0m	+5%
Case volume	15,420	24,078	30,718	26,542	36,318	31,756	-13%

Application fraud accounted for £15.6 million of card ID theft during 2016, up 11 per cent from £14.1 million during 2015.

Account take-over accounted for £24.4 million of card ID theft during 2016, up 1 per cent from £24.1 million during 2015.

2.7. Further 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 so should not be viewed as being in addition to those in the previous section. 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 to purchase goods on the high street.

2.8. UK retail face-to-face fraud

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

UK retail face-to-face fraud	2011	2012	2013	2014	2015	2016	% Change 15/16
Loss value	£43.2m	£54.6m	£60.8m	£49.5m	£53.5m	£62.8m	+17%

The majority of this fraud is undertaken using cards obtained through more basic techniques, with fraudsters finding ways of stealing both the card and PIN in order 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 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 and is a decrease on the 2015 figure of 3.6p in every £100. Fraud on contactless cards and devices represents just 1.1 per cent of overall card fraud.

2.9. UK cash machine fraud

These figures show how much fraud took place at cash machines in the UK on either stolen cards or where a card account has been taken over by a fraudster. In all cases the fraudster would need to have access to the genuine PIN and card.

UK cash machine fraud	2011	2012	2013	2014	2015	2016	% Change 15/16
Loss value	£29.3m	£28.9m	£31.9m	£27.3m	£32.7m	£43.1m	+32%

Losses at UK cash machines increased by 32 per cent to £43.1 million in 2016. However, this figure is still significantly lower than the peak of £74.6 million in 2004, prior to the rollout of Chip & PIN.

Intelligence suggests the rise is due to an increase in distraction thefts and card entrapment at ATMs, with fraudsters obtaining both the card and the PIN which enables them to commit fraud at cash machines.

2.10. Domestic / International split of total

Any fraud committed on a UK issued credit, debit or charge card used at a retailer (shop, telephone and online) based in the UK or overseas.

Domestic / International split	2011	2012	2013	2014	2015	2016	% Change 15/16
UK Fraud	£260.9m	£286.7m	£328.4m	£328.7m	£379.7m	£417.9m	+10%
International Fraud	£80.0m	£101.6m	£122.0m	£150.3m	£188.4m	£200.1m	+6%

3. Remote banking fraud

Remote banking fraud losses are collated in three categories: internet banking, telephone banking and mobile banking.

Total remote banking fraud	2011	2012	2013	2014	2015	2016	% Change 15/16
Total prevented value	N/A	N/A	N/A	N/A	£524.6m	£205.4m	-61%
Total loss value	£73.4m	£71.7m	£71.9m	£98.2m	£168.6m	£137.1m	-19%
Total case volume	N/A	23,450	19,395	21,819	33,306	33,392	0%

A total of £205.4 million of attempted remote banking fraud was stopped by bank security systems in 2016. This is equivalent to £6 in £10 of fraud attempted being prevented before a loss occurs.

The proportion of prevented fraud has reduced from £7.57 in every £10 in 2015, largely due to criminals shifting their methods away from using malware attacks on online banking systems, which bank security processes identified and stopped, and towards methods less susceptible to direct bank intervention, such as scams directly targeting the customer.

Total remote banking losses decreased by 19 per cent to £137.1 million in 2016, while the case volume remained level, indicating a lower average loss per case.

In addition, 32 per cent (£43 million) of the losses across all remote banking channels were recovered after the incident.

3.1. Internet banking fraud

This type of fraud covers fraudulent payments taken from a customer's bank account using the internet banking channel.

Internet banking fraud	2011	2012	2013	2014	2015	2016	% Change 15/16
Loss value	£51.2m	£57.0m	£58.8m	£81.4m	£133.5m	£101.8m	-24%
Case volume	N/A	16,355	13,799	16,041	19,691	20,088	+2%

Losses due to internet banking fraud fell by 24 per cent in 2016 to £101.8 million, while the number of cases increased slightly, by 2 per cent. Intelligence suggests the reduction in fraud losses is due to a decline in criminals' use of malware to target online banking systems.

In addition, 32 per cent (£32.2 million) of the losses across internet banking were recovered after the incident.

3.2. Telephone banking fraud

This type of fraud covers fraudulent payments made from a customer's bank account using the telephone banking channel.

Telephone banking fraud	2011	2012	2013	2014	2015	2016	% Change 15/16
Loss value	£22.2m	£14.7m	£13.1m	£16.8m	£32.3m	£29.6m	-8%
Case volume	N/A	7,095	5,596	5,778	11,380	10,495	-8%

Losses due to telephone banking fraud fell by 8 per cent in 2016 to £29.6 million.

In addition, 29 per cent (£8.5 million) of the losses across telephone banking were recovered after the incident.

3.3. Mobile banking fraud

This type of fraud covers fraudulent payments made from a customer's bank account specifically using a mobile banking app.

Mobile banking fraud	2011	2012	2013	2014	2015	2016	% Change 15/16
Loss value	N/A	N/A	N/A	N/A	£2.8m	£5.7m	+104%
Case volume	N/A	N/A	N/A	N/A	2,235	2,809	+26%

Losses on mobile banking fraud rose by 104 per cent to £5.7 million, with the number of cases growing at the lower rate of 26 per cent. Intelligence suggests the rise in fraud reflects customers' rising use of the channel and a larger offering of mobile banking facilities by banks.

In addition, 44 per cent (£2.5 million) of the losses across mobile banking were recovered after the incident.

4. Cheque fraud

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	2011	2012	2013	2014	2015	2016	% Change 15/16
Total prevented value	N/A	N/A	N/A	N/A	£392.8m	£196.2m	-51%
Total loss value	£38.3m	£37.6m	£31.2m	£20.2m	£18.9m	£13.7m	-28%
Total case volume	N/A	15,539	10,471	8,168	5,746	3,388	-41%

Cheque fraud losses fell by 28 per cent in 2016 to £13.7 million. This is the lowest ever annual total.

A total of £196.2 million of cheque fraud was prevented by bank monitoring systems in 2016, a 51 per cent reduction on 2015. Intelligence suggests that is due to a lower level of attack by fraudsters; however it is still equivalent to £9.40 in every £10 of attempted cheque fraud being stopped before a loss occurs.

Financial Fraud Action UK (FFA UK) is responsible for leading the collective fight against fraud in the UK payments industry. Its membership includes the major banks, credit, debit and charge card issuers, and card payment acquirers. Through industry collaboration FFA UK seeks to be the authoritative leader in defending consumers and businesses from financial fraud, by creating the most hostile environment in the world for fraudsters.

FFA UK's primary role is to drive 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. It operates its own data and intelligence sharing bureau and sponsors a fully operational police unit.

http://www.financialfraudaction.org.uk/

Follow us on Twitter: @FFAUK
Visit us on Facebook