Financial Fraud Action UK
Working together to prevent fraud

January to June 2016 fraud update: Payment cards, remote banking and cheque

October 2016

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 full fraud statistics reported by its members twice yearly. Data cover 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. 2016 half-year fraud losses

Financial fraud losses across payment cards, remote banking and cheques totalled £399.5 million in the first half of 2016. This is an increase of 25 per cent on the same period in 2015, when losses were £320.3 million.

Prevented fraud totalled £678.7 million between January and June 2016. This figure represents frauds detected and prevented by banks and card companies, equating to £6 in every £10 of fraud attempted being stopped. The proportion of prevented fraud has reduced from £7 in every £10 in the first half of 2015, due in part to fraudsters shifting their mode of attack away from using malware to steal from victims during their online banking session, and towards other forms of fraud such as vishing, smishing and other scams less susceptible to direct bank intervention.

1.2. Factors driving changes to fraud figures

It is not possible to place specific financial values on particular types of compromise or scam, but intelligence reported to FFA UK from members points to the key drivers of fraud.

Fraud continues to increase because of the growth of impersonation and deception scams and complex online attacks. All these methods target customers' personal and financial details, including card data, to facilitate fraud.

Data on the volume and value of fraud from the first half of the year suggests fraudsters are committing more offences, but stealing smaller amounts.

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

The fraudulent approach may claim there has been suspicious activity on the recipient's account or their account details need to be updated or verified. The criminal 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.

Fraudulent approaches following data breaches continue to be a driver of fraud. Data obtained during breaches can be used to commit fraud directly, such as using stolen card details. Personal and financial information obtained in a breach also can be used in scams, while the publicity around the incident itself can be used to add authenticity to any fraudulent approach.

Criminal gangs also use malware 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.

Fraud on lost and stolen cards has increased and intelligence from FFA UK members suggests there have been more incidents at ATMs, through distraction thefts and entrapment. Courier scams, in which a scammer visits the victim's house to collect either cash or a bank card, also continue to play a role in the fraud landscape.

1.3. Financial fraud data

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

Each incident of fraud referred to in this report refers to the number of accounts defrauded and not one victim of fraud. For example, a fraud carried out on two cards which belonged to the same person would represent two instances of fraud, not one.

2. Payment card fraud

This data relates to fraud on debit, credit, charge, ATM-only and prepaid 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	Jan-June 2012	Jan-June 2013	Jan-June 2014	Jan-June 2015	Jan-June 2016	% change 15/16
Total prevented value (£ millions)	n/a	n/a	n/a	355.4	475.7	34
Total loss value (£ millions)	185.0	216.1	247.6	244.6	321.5	31
Total case volume	450,983	581,170	671,388	643,500	987,299	53

Fraud losses on UK-issued cards stood at £321.5 million in the first half of 2016, up 31 per cent on the same period 2015.

Over this period, overall card spending has grown by 4.8 per cent. Card fraud as a proportion of card purchases equates to 8.7p for every £100 spent, up from 7.9p in the first half of 2015.

Banks and card companies prevented £475.7 million of card fraud in the first half of 2016, equivalent to £6 in every £10 of attempted fraud being prevented before a loss happens.

2.2. Remote purchase fraud

Remote purchase, or card not present (CNP) fraud happens when stolen payment card details are used to make a purchase on the internet, over the telephone or via mail order.

Remote purchase fraud	Jan-June 2012	Jan-June 2013	Jan-June 2014	Jan-June 2015	Jan-June 2016	% change 15/16
Total loss value (£ millions)	115.8	142.0	174.5	171.7	224.1	31
Total case volume	337,230	443,363	537,302	512,818	784,188	53

There was a 31 per cent increase in losses in the first half of 2016 compared with the same period in 2015.

While the use of card details obtained in data hacks contributed to the increase in remote purchase fraud, the growth of online retail has also given fraudsters more opportunities to use compromised personal information and card details on websites which use less secure systems.

E-commerce card fraud totalled an estimated £156.0 million, up 46 per cent compared to the first six months of 2015. At the same time, online card spending increased from £65.7 billion in the first half of 2015 to £74 billion in the same period of 2016.

Remote purchase fraud: E-commerce / Mail order and telephone order	Jan-June 2012	Jan-June 2013	Jan-June 2014	Jan-June 2015	Jan-June 2016	% change 15/16
E-commerce (£ millions)	65.6	77.6	105.4	107.3	156.0	46
Mail order and telephone order (£ millions)	50.2	64.4	69.1	64.4	68.1	6

2.3. Lost and stolen fraud

This fraud happens when lost or stolen cards are used to make a purchase (whether remotely or face-to-face), withdraw funds from an ATM or at a branch or make a bank transfer.

Lost and stolen fraud	Jan-June 2012	Jan-June 2013	Jan-June 2014	Jan-June 2015	Jan-June 2016	% change 15/16
Loss value (£ millions)	28.0	28.2	29.2	30.3	49.5	63
Case volume	54,451	65,295	66,218	65,004	115,956	78

Lost and stolen fraud losses increased 63 per cent in the first half of 2016, to £49.5 million. During this period, there has been an associated increase in incidents of distraction thefts and card entrapment at ATMs.

2.4. Card not received fraud

This type of fraud happens when a card is stolen after it has been sent but before the genuine account holder receives it.

Card not received fraud	Jan-June 2012	Jan-June 2013	Jan-June 2014	Jan-June 2015	Jan-June 2016	% change 15/16
Loss value (£ millions)	6.4	4.6	5.0	5.7	6.1	7
Case volume	4,296	4,282	4,366	5,135	5,812	13

Card not received fraud losses increased seven per cent to £6.1 million in the first half of 2016.

The increase is likely to be due to new cards being issued by card companies during the year.

2.5. Counterfeit card fraud

This refers to a fake card created by a fraudster using compromised details from the magnetic stripe of a genuine card. The details are usually stolen from a UK-issued card and used to make a fake magnetic stripe card for use overseas in countries yet to upgrade to a chip-enabled environment

Counterfeit card fraud	Jan-June 2012	Jan-June 2013	Jan-June 2014	Jan-June 2015	Jan-June 2016	% change 15/16
Loss value (£ millions)	20.2	23.3	24.1	19.8	21.3	8
Case volume	45,786	53,587	49,924	43,132	60,765	41

Counterfeit card fraud losses increased by eight per cent to £21.3 million between January and June 2016.This type of fraud remains a small proportion of overall card fraud because of the increased rollout of chip technology around the world, which has made the use of counterfeit cards difficult.

2.6. Card ID theft

There are two types of card ID theft: third-party application fraud and 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 happens when a criminal takes over a genuine card account.

Card ID theft	Jan-June 2012	Jan-June 2013	Jan-June 2014	Jan-June 2015	Jan-June 2016	% change 15/16
Loss value (£ millions)	14.6	18.1	14.7	17.1	20.6	20
Case volume	9,220	14,643	13,578	17,411	20,579	18

Application fraud accounted for £8.6million of card ID theft during the first six months of 2016, up 63 per cent from £5.2 million during the first six months of 2015.

Account takeover accounted for £12.0 million of card ID theft during the fist six months of 2016, up one per cent from £11.8 million during the same period in 2015.

2.7 Further analysis

The data in the following sections relate to the places where the card was fraudulently used, not 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 an 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. For example, a lost or stolen card could be used to make an ATM withdrawal and also purchase goods on the high street.

2.8 UK retail face-to-face fraud

UK retail face-to-face fraud includes all transactions occurring face-to-face in a UK shop, excluding contactless transactions.

UK retail face-to-face fraud	Jan-June 2012	Jan-June 2013	Jan-June 2014	Jan-June 2015	Jan-June 2016	% change 15/16
Loss value (£ millions)	26.5	27.2	35.9	23.6	28.9	22

This fraud tends to be a result of fraudsters who have stolen a card and PIN committing fraud in shops. Cards and PINs are obtained through ATM-related crimes such as distraction thefts, card entrapment and shoulder surfing, as well as scams in which victims give their cards to fraudsters. Fraudsters also obtain them via intercepting new cards in the post and through third-party applications.

Contactless frauds are contactless payments on cards or devices which have been fraudulently obtained or through first-party fraud. These incidents take place in retail environments; there has never been a confirmed real world case of a contactless card being scanned remotely for either its details or a payment. Contactless fraud remains low with £2.9 million of losses during the first half of 2016, compared to spending of £9.27 billion over the same period. This is equivalent to 3.1p in every £100 spent using contactless technology and is a decrease on the 2015 full-year figure of 3.6p. Fraud on contactless cards and devices is less than one per cent of overall card fraud.

2.9 UK cash machine fraud

This is fraud at UK ATMs using stolen cards or cards from an account which has been taken over by a fraudster. A fraudster would need the genuine PIN and card to make a withdrawal.

UK cash machine fraud	Jan-June 2012	Jan-June 2013	Jan-June 2014	Jan-June 2015	Jan-June 2016	% change 15/16
Loss value (£ millions)	14.6	16.2	14.3	14.9	20.6	38

Losses at UK cash machines increased by 38 per cent during the first six months of 2016, but remains much lower than before the introduction of Chip & PIN.

2.10 Domestic / international split of total

This is fraud committed on a UK-issued credit, debit, charge or ATM-only card used at a retailer (in face-to-face and remote environments) based in the UK or overseas.

Domestic / international split	Jan-June 2012	Jan-June 2013	Jan-June 2014	Jan-June 2015	Jan-June 2016	% change 15/16
UK fraud (£ millions)	138.9	155.9	175.2	167.5	215.2	28
International fraud (£ millions)	46.1	60.2	72.4	82.4	106.3	29

3. Remote banking fraud

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

Total remote banking fraud	Jan-June 2012	Jan-June 2013	Jan-June 2014	Jan-June 2015	Jan-June 2016	% change 15/16
Total prevented value (£ millions)	N/A	N/A	N/A	293.5	103.2	-65
Total loss value (£ millions)	34.3	31.7	47.8	66.2	70.6	7
Total case volume	11,674	9,566	10,908	13,971	17,687	27

Overall remote banking loses increased by seven per cent to £70.6 million in the first half of the year. While losses are still increasing, the rate is slowing year-on-year due to improved banking security systems and as a result of fraud prevention work by the industry. By contrast, the increase between the first six months of 2014 and 2015 was 38 per cent.

Remote banking fraud continues to be caused by impersonation and deception scams. Criminals dupe their victim into giving away their personal and security details and use these details to gain access to their victim's bank account. Increasingly, businesses and high-net-worth customers are being targeted by fraudsters.

A total of £103.2 million of attempted remote banking fraud was stopped by bank security systems. This is equivalent to £5.9 in £10 of fraud attempted being prevented before a loss happens. The amount of fraud prevented has declined in part to fraudsters shifting their mode of attack away from using malware to steal from victims during their online banking session, and towards other forms of fraud such as vishing, smishing and other scams less susceptible to direct bank intervention.

In addition, 37 per cent (£26.2 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 via internet banking.

Internet banking fraud	Jan-June 2012	Jan-June 2013	Jan-June 2014	Jan-June 2015	Jan-June 2016	% change 15/16
Loss value (£ millions)	26.4	25.5	40.4	50.4	55.3	9
Case volume	8,323	6,770	8,150	8,417	11,195	33

Internet banking fraud losses increased by nine per cent to £55.3 million in the first half of 2016. The introduction of new security systems by banks has seen the growth rate of losses reduce but bank accounts continue to be a target for fraudsters, who are targeting the customer and duping them to give away their passcodes.

Some 37 per cent (£20.4 million) of the losses across internet banking were recovered after the incident.

3.2. Telephone banking fraud

This typically involves fraudsters duping customers into providing their telephone banking details, in order to impersonate them and make payments from the victim's account to one they control, through phone calls, text messages or online.

Fraudsters may also use this information to make changes to a victim's account to commit fraud via other means such as online banking, in what is known as a cross-channel attack.

Internet banking fraud	Jan-June 2012	Jan-June 2013	Jan-June 2014	Jan-June 2015	Jan-June 2016	% change 15/16
Loss value (£ millions)	7.9	£6.2	7.4	14.7	13.1	-11
Case volume	3,351	2,796	2,758	4,777	4,949	4

Telephone banking losses fell by 11 per cent to £13.1 million in the first half of 2016, despite a four per cent increase in cases. The decline in losses again reflects enhanced security systems by banks, now increasingly using voice biometrics for telephone banking customers.

Some 37 per cent (£4.9 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. This type of fraud is not very common and with only two years' data available it is not possible to draw conclusions about trends.

Mobile banking fraud	Jan-June 2012	Jan-June 2013	Jan-June 2014	Jan-June 2015	Jan-June 2016	% change 15/16
Loss value (£ millions)	N/A	N/A	N/A	1	2.2	120
Case volume	N/A	N/A	N/A	777	1,543	99

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 a 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 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	Jan-June 2012	Jan-June 2013	Jan-June 2014	Jan-June 2015	Jan-June 2016	% change 15/16
Total loss value (£ millions)	19.2	16.9	12.0	9.5	7.4	-22
Total case volume	8,142	5,284	4,784	2,837	2,108	-26

Cheque fraud losses fell by 22 per cent to £7.4 million in the first six months of 2016, continuing a downwards trend and the lowest six month total ever reported.

Bank monitoring systems stopped £99.8 million of attempted cheque fraud in the first half of the year. This is equivalent to £9.30 in every £10 of attempted cheque fraud being stopped before a loss happens.

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

FFA UK is leading Take Five, a national campaign that offers straightforward and impartial advice to help everyone protect themselves from preventable financial fraud. This includes email deception and phone-based scams as well as online fraud – particularly where criminals impersonate trusted organisations. It 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.

https://takefive-stopfraud.org.uk/

Follow Take Five on Twitter: @takefive
Visit us on Facebook

The Dedicated Card and Payment Crime Unit (DCPCU) is a unique proactive police unit, with a national remit, formed as a partnership between Financial Fraud Action UK, the City of London Police and the Metropolitan Police together with the Home Office. It is fully sponsored by the cards and banking industries, with an on-going brief to investigate, target and, where appropriate, arrest and seek successful prosecution of offenders responsible for card, cheque and payment fraud crimes. It is headed up by a Detective Chief Inspector and comprises officers from the Metropolitan and City of London police forces who work alongside banking industry fraud investigators and support staff.

The UK Cards Association is the trade body for the card payments industry in the UK, representing financial institutions which act as card issuers and acquirers. Members of the Association account for the vast majority of debit and credit cards issued in the UK - issuing in excess of 59 million credit cards and 98 million debit cards - and cover the whole of the payment card acquiring market.

The Association promotes co-operation between industry participants in order to progress non-competitive matters of mutual interest; informs and engages with stakeholders to

shape legal and regulatory developments; develops industry best practice; safeguards the integrity of the card payments industry by tackling card fraud; develops industry standards; and co-ordinates other industry-wide initiatives such as those aiming to deliver innovation. As an Association we are committed to delivering a card payments industry that is constantly focused on improved outcomes for the customer.
www.theukcardsassociation.org.uk

The Cheque and Credit Clearing Company (C&CCC) is a non-profit making industry body, which has managed the cheque clearing system in England and Wales since 1985, and in all of Great Britain since 1996 when it took over responsibility for managing the Scottish cheque clearing. As well as clearing cheques, the system processes bankers' drafts, postal orders, warrants, government payable orders and travellers' cheques.

The company also manages the systems for the clearing of paper bank giro credits (the credit clearing), euro cheques (the euro clearing) and US dollar cheques (the currency clearing for US dollar cheques drawn on London banks).

To ensure the long-term future of cheques for consumers, charities and businesses, the C&CCC is introducing cheque imaging in the UK and is now working with the banking industry to agree the necessary changes to the infrastructure and technological changes required. For more information visit
www.chequeandcredit.co.uk/cheque_and_credit_clearing/cheque_imaging/