## CONTENTS

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Foreword</td>
</tr>
<tr>
<td>7</td>
<td>What we do</td>
</tr>
<tr>
<td>9</td>
<td>2014 at a glance</td>
</tr>
<tr>
<td>10</td>
<td>Snapshot on fraud</td>
</tr>
<tr>
<td>13</td>
<td>The fight against fraud: headline figures and trends</td>
</tr>
<tr>
<td>19</td>
<td>The fraud prevention agenda</td>
</tr>
<tr>
<td>21</td>
<td>Education and awareness campaigns</td>
</tr>
<tr>
<td>25</td>
<td>Promoting data and intelligence-sharing</td>
</tr>
<tr>
<td>29</td>
<td>Industry-funded police unit</td>
</tr>
<tr>
<td>33</td>
<td>Joining forces with partners, including government</td>
</tr>
<tr>
<td>35</td>
<td>Further services and activity</td>
</tr>
</tbody>
</table>
2014 was a year of change for the payments industry, much of it driven by the need to adapt to the regulatory reform affecting the financial services sector more widely. Against this background, the fraud landscape continues to evolve, with new threats emerging and an even greater premium on collaborative action to address risks to customers.

In response, we have been working with government to ensure that the legal and regulatory framework is as conducive as possible to facilitating fraud prevention at both UK and European level. In doing so, we have been providing an industry-wide voice to shape a favourable environment for members’ businesses, particularly as their resources are stretched.

Over the year we examined our governance, structure and activities to ensure the best possible value for members, while making sure our objectives and role in the crowded landscape are clearly delineated and understood. A key driver was the acknowledged need to deal with financial fraud in a more holistic and co-ordinated way, adopting a pan-industry approach to reflect the way in which fraudsters are coordinating attacks against the industry. Consequently, members felt it was time to establish a senior fraud strategy body to provide a strong, clearly defined governance structure and ensure clarity, accountability and objectivity in the way fraud is managed across the industry.

I am pleased to say that, as a result, FFA UK recently (April 2015) became an incorporated body and has held its first FFA UK Board meeting. Our committee structure has been streamlined to help meet the changing requirements of the industry. We have also been given a wider remit that encompasses first and third party fraud on all core banking products/services, channels and both personal and business customers. (For more details, see ‘What we do’).

As FFA UK has reconfigured itself for the future, the wider fraud landscape has been fast-moving. Our industry came under scrutiny at the end of 2014 at the Treasury Select Committee where there were suggestions of underreporting. FFA UK members were quick to respond by agreeing to publish for the first time the numbers of fraud incidents so that the dynamics of the fraud environment in the UK can be more fully understood. There is also commitment during the coming year to consider compiling other metrics which might shine a light on the scale of financial fraud in the UK.
Looking across the fraud landscape, efforts by criminals to dupe customers into giving away their personal and financial details show no signs of abating. Worryingly, incidents where customers are convinced by fraudsters over the phone that they are talking to the bank or the police appear to be increasing. This is an insidious crime, often targeting the elderly and vulnerable. It was industry concern about these attacks that drove a major campaign in December 2014, which had at its centre the FFA UK-coordinated Joint Declaration of the UK Banks, which highlighted some clear messages about things you will never be asked to do over the phone by the bank or the police. Supported by the Association of Chief Police Officers, the Financial Conduct Authority and by the Home Office Minister Karen Bradley, the campaign achieved widespread coverage.

Successful though this was, it has become clear that such campaigns can only be a starting point when it comes to raising awareness and changing behaviour amongst the public. A much more concerted effort is needed, delivering key messages to customers as often and in as many channels as possible. It is also clear that this is not just a banking industry problem, with fraudsters also posing as officials from public bodies including HM Revenue and Customs, and private sector organisations such as computer companies, to deceive consumers and businesses into parting with their money. During 2015, FFA UK will join forces with the many industries and sectors touched by this fraud to create a genuine step change in consumer awareness and prevention. Will you join us?

“The UK Cards Association is proud of its continuing role as the main sponsor of Financial Fraud Action UK (FFA UK). FFA UK’s programme is having a marked impact, with high-profile consumer awareness work backed by a strong enforcement arm through the Dedicated Card and Payment Crime Unit (DCPCU). In particular, our police colleagues have delivered incredibly strong results for the industry over the last year.”

GRAHAM PEACOP, MANAGING DIRECTOR OF THE UK CARDS ASSOCIATION
WHAT WE DO

Financial Fraud Action UK (FFA UK) is responsible for leading the collective fight against fraud in the UK payments industry. Our membership includes banks, credit, debit and charge card issuers, and card payment acquirers in the UK. We provide a forum for our members to work together on non-competitive issues relating to financial fraud.*

Our 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

We do this by:

- Sponsoring the Dedicated Card and Payments 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 the Industry Strategic Threat Management Process, which provides an up-to-the-minute picture of the threat landscape
- Delivering UK-wide awareness campaigns to inform customers about threats and how to stay safe
- Managing intelligence-sharing through the industry fraud intelligence hub (Financial Fraud Bureau) and the Fraud Intelligence Sharing System (FISS) which feeds intelligence to police and other agencies in support of law enforcement activity
- Informing commentators and policy-makers through a press office and public affairs function
- 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

Key partner

FFA UK works in partnership with The UK Cards Association (UK Cards) 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. Members of the Association account for the vast majority of debit and credit cards issued in the UK – issuing in excess of 55 million credit cards and 95 million debit cards – and cover the whole of the payment card acquiring market.

*Financial fraud includes first and third 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).
2014 AT A GLANCE

- **JAN** The ‘Out of Your Hands’ package was launched – an online resource introduced by FFA UK and the Telecommunications UK Fraud Forum to raise awareness amongst young people of the need to stay safe online.

- **FEB** Launched HM Government’s Cyber Streetwise campaign, which FFA UK supported as a funding partner. The programme is focused on raising public awareness of scams which target consumers by e-mail and over the internet.

- **MAR** Morrisons Supermarket suffered a data breach of 100,000 employee payroll records. In response, FFA UK’s Financial Fraud Bureau (FFB) worked against the clock to ensure that action could be taken to protect customers’ accounts.

- **APR** Tony Colston-Hayter, the head of an internet gang which stole £1.25m from banks, was sentenced to five and a half years imprisonment following a witness statement provided by the FFB.

- **MAY** After a two year investigation by the DCPCU, two fraudsters were sentenced to four years each at The Old Bailey for stealing over £1m from customers’ accounts.

- **JUN** Courier Fraud Awareness Day saw the DCPCU working in close partnership with the banks and consumer bodies. DCPCU’s Fraud Prevention Officer appeared on BBC’s Watchdog programme.

- **JUL** Forensic funding from the FFB helped put two fraudsters in jail for 14 years.

- **AUG** The DCPCU-led international alliance behind Operation Sandhaven secured the conviction of an organised criminal gang responsible for major ATM fraud, with members receiving a total of 15 years in prison.

- **SEP** FFA UK delivered a ‘biometric in banking’ workshop on behalf of the European Association of Biometrics (EAB)

- **OCT** Two ringleaders of one the UK’s largest ever fraud cheque gangs were sentenced to a total of 18 years in prison at Bradford Crown Court in October. During the DCPCU led operation to investigate and arrest the pair, almost 3,000 stolen or fake cheques were seized, which together had a value of £6.5m.

- **NOV** An online video was launched by FFA UK, as part of HM Government’s Cyber Streetwise campaign, which sets out the steps businesses can take to protect themselves when accepting card payments online.

- **DEC** A UK-wide ‘Day of Action’ was declared by FFA UK to raise awareness of common telephone frauds, amongst the public and advise them how to beat the criminals. As part of this, a Joint Declaration of the UK Banks, Card Issuers and Building Societies was launched.
SNAPSHOT ON FRAUD

Since 2002, DCPCU has:

- Achieved £470m savings from reduced fraud
- Saved the industry the equivalent of over £800,000 per week
- Upheld a conviction rate of 94%
- Secured 415 convictions on fraud related matters

High street card fraud losses

- 2014 high street card fraud losses are £49.2m
- 2004: £153,000, 12.4p for every £100
- 2008: £2.32bn, 12% of respondents in a similar study carried out in 2013
- 2014: £148bn, 7.5p for every £100

The amount of fraud as a proportion of the amount spent on cards during 2014 compared with 2008 was:

- 2004: 78% since the introduction of Chip & PIN in 2004
- 2008: 9.2p was fraudulent for every £100 spent online
- 2014: 0.7p for every £100 spent on contactless cards
Since 2002, DCPCU has:

- High street card fraud losses saved the industry the equivalent of over £49.2m.
- Upheld a conviction rate of 2014 high street card fraud losses are £470m.
- Achieved savings from reduced fraud of £49.2m.
- Secured convictions on fraud related matters of people have received a call that seemed suspicious.

The amount of fraud as a proportion of the amount spent on cards during 2014 compared with 2008 was:

- A fall of 94% since the introduction of Chip & PIN in 2004.

Fraud on contactless cards remains very low:

- Only 1 in 1000 remote purchase transactions are fraudulent.
- 12% reduction in phishing websites during 2014.
- 58% of people have received a call that seemed suspicious.

A steep rise from 41% of respondents in a similar study carried out in 2013.

E-commerce spend on cards in UK in 2014 was £148bn.

- This represents just 0.7p in every £100 spent on contactless.
- For every £100 spent online...
- ... only 9.2p was fraudulent.

Fraud on contactless cards remains very low:

- Just £153,000 of losses over 2014 compared with total spending of £2.32bn.
FFA UK collates fraud loss statistics across the payments industry to produce a range of reports for its members. The losses are reviewed and analysed, with findings feeding into the Industry Strategic Threat Management Process to shape the fraud prevention work programmes.

FFA UK also publishes industry fraud figures twice a year. During 2014 FFA UK undertook a comprehensive review of its reports, resulting in a revised suite of enhanced reports which are being rolled out during 2015.

The following information captures the latest headline figures on fraud losses across all channels.

**Card fraud**

Fraud losses on UK cards totalled £479m in 2014, a 6% rise on the 2013 figure of £450m. This is still 21% lower than the peak of £609.9m back in 2008. By way of comparison, the overall value of card transactions across the UK increased by 5 per cent to £802bn. Card fraud losses as a proportion of the value of purchases has risen slightly from 7.4p in every £100 spent, to 7.5p in 2014. In 2008, this was 12.4p in every £100. Overall, the number of incidents of card fraud rose by 5 per cent to 1.3m in 2014.

Losses on purchases made using a card remotely – those made online, over the phone or by mail order – rose 10% in 2014 to £331.5m. The number of incidents rose 7% from the previous year. Contained within these figures, e-commerce card fraud losses increased from £190.1m in 2013 to £217.4m in 2014 – a 14% rise. For the first time FFA UK has compiled sales figures for remote purchases. In 2014 e-commerce spending in the UK was £148 billion, meaning that for every £100 spent only 9.2p was fraudulent.

Losses declined at both UK retailers and UK ATMs, with decreases of 14% to £49.2m and 15% to £27.3m respectively.

**Fraud losses on UK-issued cards, 2004 to 2014**

![Bar chart showing fraud losses on UK-issued cards from 2004 to 2014](chart.png)
The overall increase in card fraud losses was driven by criminals using UK cards fraudulently abroad, which increased by 23% to £150.3m. Domestic card losses remained flat at £328m. A key reason for rising levels of fraud abroad on UK cards is that criminals circumvent their security features when using them in overseas locations.

These trends owe much to the growth of deception crimes, as well as sophisticated online attacks such as malware and data hacks, to compromise card details. In response, the industry continues in its efforts to warn consumers and retailers to install security software which is often freely available from their banks. There are a number of other initiatives in place for consumers and businesses to tackle this type of activity including; Address Verification Service (AVS), Card Security Code (CSC) and the extra layer of verification checking for online transactions offered by the three card schemes – American Express SafeKey, MasterCard SecureCode and Verified by Visa.

Fraud on contactless cards remains very low, with just £153,000 of losses over 2014 compared with total spending of £2.32bn. This represents just 0.7p in every £100 spent on contactless.
Online banking fraud
Online banking fraud increased from £40.9m to £60.4m in 2014, a 48% rise. More encouragingly, the number of confirmed online banking fraud loss incidents was just 53,192, a number which is relatively modest considering the Office for National Statistics (ONS) report that 53% of UK adults now use online banking, which equates to 26.9 million users.* It is also 16% down on the 2010 high of 63,623.

A driver for this type of crime is the surge in organised criminal gangs’ use of malware (malicious software which is unknowingly downloaded onto a computer) and ‘phishing’ emails as a means to compromise online banking customers’ security credentials. Once obtained, fraudsters will use these details to access customers’ accounts, often transferring funds into a beneficiary account – otherwise known as a money-mule account. From there, the funds are transferred quickly through several accounts, and often out of the country.

Due to the sophisticated and organised nature of this crime, customers can find it difficult to differentiate between legitimate communication from their bank, or other legitimate service provider, and false approaches from criminals. While traditional phishing attacks using the banks’ brands reduced during 2014, reports of phishing and other emails containing malicious attachments using other brands, such as HM Revenue and Customs, have increased. Criminals continue to employ novel techniques to infect devices and deceive customers into divulging sensitive information that can then be used to commit fraud.

Telephone-based deception crimes have also been a big factor driving recent increases. Online banking customers are being tricked into divulging their login details, passwords and other personal data over the telephone to a caller they believe is from their bank or the police, but who is actually a fraudster.

*www.ons.gov.uk/ons/dcp171778_373584.pdf
Telephone banking fraud
Telephone banking fraud losses increased 20% from £11.6 million in 2013 to £13.9 million in 2014. The methods used to compromise customers’ credentials mirror those used to commit banking fraud online, but these are then used to access customers’ accounts via telephone banking.

Cheque fraud
Cheque fraud losses fell 35% to £17.8 million in 2014 from £27.5 million the previous year. This is the lowest loss ever reported in this category. The decrease is owed not only to diminishing volumes of cheques being written by UK consumers and businesses, but also to the positive impact of more sophisticated fraud detection.

Online and telephone banking fraud net losses

<table>
<thead>
<tr>
<th>Year</th>
<th>Online Banking</th>
<th>Telephone Banking</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>12.2</td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td>23.2</td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td>33.5</td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>22.6</td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>52.5</td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td>59.7</td>
<td>12.1</td>
</tr>
<tr>
<td>2010</td>
<td>46.7</td>
<td>12.7</td>
</tr>
<tr>
<td>2011</td>
<td>35.4</td>
<td>16.7</td>
</tr>
<tr>
<td>2012</td>
<td>39.6</td>
<td>12.6</td>
</tr>
<tr>
<td>2013</td>
<td>40.9</td>
<td>11.6</td>
</tr>
<tr>
<td>2014</td>
<td>60.4</td>
<td>13.9</td>
</tr>
</tbody>
</table>

Telephone banking fraud losses were not collected before 2009.
systems in use across the industry. The overwhelming majority of this type of fraud is stopped before the cheque is paid: In fact 94% of all attempted cheque fraud was spotted and prevented during the clearing process in 2014.

More information on fraud volumes and values, as well as preventative activity and advice is available through the publication Fraud the Facts, which can be downloaded free of charge from the FFA UK website www.financialfraudaction.org.uk/joint-declaration-phone-scams.asp
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 and so is 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.

The following chapter sets out the activity across the following key strands:

- Education and awareness campaigns
- Promoting data and intelligence sharing
- Industry funded police unit
IMPORTANT INFORMATION FOR ALL UK BANK CUSTOMERS

Fraudsters are increasingly targeting consumers over the telephone, posing as bank staff, police officers and other officials or companies in a position of trust. Often the fraudster will claim there has been fraud on your account and that you need to take action.

Your bank or the police will never:
- Phone you to ask for your 4-digit card PIN or your online banking password, even by tapping them into the telephone keypad.
- Ask you to withdraw money to hand over to them for safe-keeping.
- Ask you to transfer money to a new account for safe-keeping, even if they say it is in your name.
- Send someone to your home to collect your cash, PIN, payment card or cheque book if you are a victim of fraud.
- Ask you to purchase goods using your card and then hand them over for safe-keeping.

If you are given any of these instructions, it is a fraudulent approach. Hang up, wait five minutes to clear the line, or where possible use a different phone line, then call your bank or card issuer on their advertised number to report the fraud.

Your bank will also never ask you to check the number showing on your telephone display matches their registered telephone number. The display cannot be trusted, as the number showing can be altered by the caller.
A key priority for FFA UK is to raise awareness amongst consumers and businesses about how to protect themselves from fraud. We achieve this by delivering impactful national awareness campaigns specifically targeted at key vulnerable groups, often in conjunction with like-minded partners.

**Telephone scams – Joint Declaration of the UK Banks**

In December, FFA UK launched a major UK-wide ‘Day of Action’ on phone scams, with the intention of raising awareness of common telephone frauds and advising the general public on how to beat the criminals. This follows an increase in the prevalence of scams in which a criminal, while making a phone call to a potential victim, poses as a representative of a trusted organisation such as a bank or the police. The fraudster will then typically attempt to obtain personal or financial information, such as the four digit PIN, or convince the individual to transfer money from their accounts.

The campaign was backed by a range of organisations including the Financial Conduct Authority, Association of Chief Police Officers, Which?, Citizens Advice, Neighbourhood Watch and the Money Advice Service – all of whom promoted the campaign’s key messages. The campaign included a Joint Declaration by the UK banks, building societies and card issuers, which set out requests banks will never make of customers over the telephone. The Joint Declaration featured as an advert across a range of national newspapers, and its launch received wide coverage across television, radio and the press.

Following its conclusion we conducted research to measure its success and encouragingly it found that 40% of the population had noticed our campaign. Asked if the advice improved their understanding about how to tell the difference between a genuine and fraudulent telephone call, 83% said it had made a positive difference and 39% said that they now felt more confident in protecting themselves against phone scams having seen our campaign.
Out of Your Hands
School pupils are often the first to use new technology, which brings with it potential new risks. Meanwhile, the popularity of social media has meant that most young people are used to sharing their personal data online – information which in criminal hands could put them at risk of identity theft and fraud. FFA UK joined forces with the Telecommunications UK Fraud Forum (TUFF) to teach young people (aged 7 to 16) about the responsible way to operate and safeguard a mobile phone, as well as the value of personal information and how to protect it. The programme created a wider focus on the importance of online security and gave advice about how to avoid becoming a victim of fraud.

‘Out of Your Hands’ (www.outofyourhands.com) was launched in January 2014, and is a teaching resource aligned to the National Curriculum which features examples of typical fraud scams, mobile phone crime and guidance on how to stay safe when making online transactions. Additionally, the package provides real-life victim and perpetrator case studies and short films. The intention of the resource is to raise awareness of scams, and help young people consider the risks of sharing their personal information with others.

Small businesses campaign
FFA UK developed a collaborative campaign to raise awareness amongst businesses of the dangers of social engineering – particularly phone scams and invoice fraud. Posters and leaflets and a social engineering education pack (designed to be used in training workshops for business staff, accompanied by a number of different cases studies to bring the themes to life) were developed for use by businesses. Bodies such as the Federation of Small Businesses, British Chambers of Commerce, National Farmers Union and Chartered Institute of Public Finance and Accountancy were engaged to make arrangements to distribute the posters, leaflets and the education pack amongst businesses using their channels.
EDUCATION AND AWARENESS CAMPAIGNS

‘Scam Alerts’ and media handling
Our press office delivers coverage for awareness campaigns and publicity for DCPCU operations, as well as providing a full reactive service dealing with enquiries from national, local and specialist media. In 2014 we launched a new series of Scam Alerts, warning the public of developing fraud trends such as telephone number spoofing and invoice fraud. Last year, we responded to over 690 media enquiries covering fraud and card payment issues, secured over 2,390 pieces of media coverage and conducted 195 broadcast interviews.

HM Government’s Cyber Streetwise campaign
FFA UK provided input as a funding partner towards the development of the Cyber Streetwise campaign, which was launched in January 2014. This ongoing national programme aims to measurably improve the online safety behaviour and confidence of consumers and small businesses. The campaign website (www.cyberstreetwise.com) includes a wealth of simple advice, as well as links to resources to help individuals, their families, and businesses, protect themselves online.

In December 2014, as part of the Cyber Streetwise campaign, FFA UK launched an online video setting out the steps businesses can take to protect themselves when accepting card payments online. The 40 second online animation, which received over 180,000 views within the first month of its launch, emphasises the importance of ‘Knowing Your Customer’ and using online authentication when taking card payments over the internet.
Pulling together fraud intelligence is like holding pieces of a jigsaw. Organisations may hold individual pieces of the jigsaw which mean little on their own. However, when all the pieces are put together, the picture can be built quickly, preventative action can be taken and organised criminal gangs can be identified for disruption and law enforcement activity.

A key strand of FFA UK’s programme is to act as a conduit for data & intelligence-sharing across the payments industry, and beyond with partners including the police. The coordination that is made possible through our Fraud Intelligence Sharing System (FISS) also allows us to share insights, where appropriate, with other agencies, including the National Crime Agency, the National Fraud Intelligence Bureau (NFIB) and the Cabinet Office’s Counter Fraud Checking Service.

Critical aspects of FFA UK’s intelligence-sharing work include the following:

**Financial Fraud Bureau (FFB)**

FFB is the industry’s intelligence hub. The unit plays an important role by leading the industry’s collective initiatives on fraud intelligence-sharing between the banks, card companies and their key partners. Its primary roles are:

- Gathering, collating and analysing the intelligence that informs the Industry Strategic Threat Management Process and providing the payments industry’s input into national threat assessments
- Disseminating intelligence directly from, and to, police forces and other law enforcement organisations, as well as the banks
- Working closely with the industry funded police Unit (DCPCU – see page 29), the National Fraud Intelligence Bureau (NFIB), and the National Crime Agency (NCA) as well as other law enforcement agencies
- Managing the Fraud Intelligence Sharing System (FISS)
- Issuing and receiving intelligence alerts from the payments industry and a wide range of other stakeholders

On a regular basis, members share intelligence with each other, and with law enforcement agencies, on issues including new scams against their customers and associated counter measures.

**Morrisons data breach**

On the morning of Friday 14th March, Morrisons Supermarket suffered a data breach of 100,000 payroll records of their employees. In response, staff at the Financial Fraud Bureau (FFB) worked against the clock to protect members through a huge, swift fraud intelligence-sharing exercise, with the aim of ensuring that action could be taken to protect customers’ accounts.

After making pro-active contact with Morrisons, FFB created a secure transfer capability and received the relevant data. The matching process took considerable time due to the volume of data, but in a couple of hours all data had been processed and disseminated, not only to FFA UK members but to the Building Societies and British Bankers Association who had been warned to expect the data. The effect was that protections were put in place to safeguard customers’ finances.
**FFB helps secure cyber gang conviction**

In April, Tony Colston-Hayter, the head of an internet gang which stole £1.25m from banks, was sentenced to five and a half years imprisonment in recognition of the seriousness of his crimes. The witness statement provided by the FFB played a major role in demonstrating the seriousness of the offence.

The trial heard that Hayter and nine others used a ‘Trojan Horse’ device to hijack computers at branches of several major banks, resulting in card details from about one million intercepted letters being stolen between 2012 and 2013. A KVM (keyboard, video, mouse) device was also used to control accounts and make 128 transfers worth over a million pounds.

The Metropolitan Police eCrime Unit (PeCU) thanked members for contributing, through FFA UK, to one of the biggest cases the Unit has dealt with to date.

The officer in charge wrote:

“Today’s conviction has struck a major and decisive blow against this global cyber-crime gang. Quite what they have managed to steal is yet to be determined but their conviction has prevented them from systematically defrauding thousands more bank customers across the world. This is by far the biggest case the Police e-Crime Unit (PeCU) has dealt with to date and is likely to be the biggest cyber phishing case so far in the UK. Thanks to the FFA UK and all members who assisted in this investigation.”

The outcome of this case highlights the value delivered by FFB’s work in producing witness statements in support of fraud convictions.

---

**Financial Fraud Desk within the NFIB**

During the year the FFB has been working with the National Fraud Intelligence Bureau (NFIB) within the City of London Police to identify the organised crime groups attacking across the industry, with a view to disrupting their activity.

Working alongside the NFIB has increased the level of analytical material available to the FFB, and has widened access to intelligence sources. This has helped the team identify viable lines of enquiry which would not otherwise have been available to the FFB. The effect of this has been an increase in police investigations being taken forward.
Fraud Intelligence Sharing System (FISS)

FISS is our central industry database – an extremely secure, flexible and cost-effective intelligence system designed to support the card and retail banking industries in the fight against fraud. It can be used to identify linkages and patterns in frauds, insights from which support the police, thereby playing an important role in protecting consumers. Members submit a range of information on fraud, which offers the benefit of sector-wide intelligence in a flexible format. This helps the industry and the police tackle those responsible and strengthen the defences. Importantly, the system allows us to supply fraud data and intelligence collated by the payments industry to the National Fraud Intelligence Bureau (NFIB), which informs law enforcement activity in the UK.

Some 2014 stats from FFB

- 333,458 cards at risk circulated
- 127 intelligence alerts issued
- 25 funded forensic police operations

Sharing intelligence with public agencies

FFA UK has extended this collaborative data-sharing beyond our sector, in the wider national interest, joining with others who share our strategic concern in eliminating fraud. A major priority for the government, driven by the Cabinet Office, is to create a step-change in the amount of intelligence shared between the public and private sectors, with a view to coordinating joint action against fraudsters. FFA UK has led the industry’s response to this agenda by contributing to the national Intelligence Sharing Roadmap, the aim of which is to tackle criminals who work in an organised way to exploit the vulnerabilities across different systems and industries.
The Dedicated Card and Payment Crime Unit (DCPCU) is a special police unit that consists of police officers from the City of London and Metropolitan Police Service who work alongside industry fraud investigators. Established in April 2002, the unit is fully sponsored by the payments industry which invests nearly £3.4 million per year in its operation.

The DCPCU’s national remit is to identify and target the organised criminal gangs responsible for card and payment crime. Since its inception in 2002, the unit has:

- Achieved £470 million in savings from reduced fraud – with the current level of savings equivalent to over £800,000 per week
- Recovered 75,000 counterfeit cards
- Recovered 596,000 compromised card numbers
- Secured 415 convictions on fraud related matters
- Upheld a conviction rate of 94%

Since 2002, DCPCU has:

- Saved the industry the equivalent of over £800,000 per week
- Achieved £470 million savings from reduced fraud
- Upheld a conviction rate of 94%
- Secured 415 convictions on fraud related matters
Examples of key operations

Operation Puccini
Two ringleaders of one the UK’s largest ever fraud cheque gangs were sentenced to a total of 18 years in prison at Bradford Crown Court in October.

Onais Hove, 43, of Barnsley and Charles Nyongo, 43, of Hunslet, Leeds, led an organised criminal gang that intercepted genuine cheques in the post which they then altered and cashed into accounts they controlled. They also photographed blank cheque books to record legitimate details which in turn were used to create fake cheques.

During the DCPCU led operation to investigate and arrest the pair, almost 3,000 stolen or fake cheques were seized, which together had a value of £6.5m. The gang’s criminality began in Scotland before spreading throughout the rest of the country. In total, eight police forces co-ordinated their work to investigate and raid the gang’s operation.

Operation Sandhaven
On 21 August, an organised criminal gang was sentenced to a total of fifteen years in jail for major ATM fraud at The Old Bailey.

Florin Ioan Silaghi, Vasile Daniel Pop, Ovidiu Metac, and Adriana Alexandra Turc were arrested in December at a property in Harrow, Middlesex where officers found a wide array of equipment used to commit fraud, including card skimmers, cards traps, cloned cards and spy cameras. The card details of 60,000 people were recovered at the property – of these, 36,000 were from cards belonging to UK residents, representing a total street value of £16m. The gang was successfully prosecuted after an extensive investigation by the DCPCU with assistance from the Romanian National Police.

Supporting wider law enforcement
FFA UK’s intelligence unit [the Financial Fraud Bureau] interacts with police forces and law enforcement agencies on a daily basis. The Bureau acts as a conduit on industry investigations ensuring de-confliction between forces and agencies, while also delivering intelligence promptly to support investigations.

During 2014, FFB supported the virtual task force of the National Cyber Crime Unit (NCCU) and the Economic Crime Command of the National Crime Agency in combatting money mules – members of the public who allow their account to be used to launder the proceeds of fraud.

The industry welcomed the launch of the Metropolitan Police fraud response unit Falcon, which presents an opportunity to collaborate further on investigations relating to the organised criminal gangs behind the fraud.

Another key piece of work during 2014 was around the quantification of cybercrime attacks against the banking industry. For a number of years the industry and external stakeholders such as law enforcement and government have tried to ascertain an accurate figure on the cost of cybercrime. This
DCPCU on BBC Watchdog

As part of Courier Fraud Awareness Day, Tony Blake, the DCPCU Fraud Prevention Officer appeared on BBC Watchdog to explain how the scam works and how people can avoid falling victim. The courier fraud scam works by the fraudsters convincing consumers to hand over their card, or move money into another account if requested to do so by a criminal purporting to be from their bank. Speaking to host Anne Robinson live in the studio, Tony Blake discussed the work police and banks are doing with telephone companies to drastically cut the time for which fraudsters can keep phone lines open – this work is a crucial element in combatting the crime.

The press office also arranged for a case study element. This segment was particularly powerful because Mary Berners-Lee appeared an unlikely victim of courier fraud. Ms Berners-Lee is the mother of Sir Tim Berners-Lee, the internet pioneer, as well as a renowned scientist in her own right.

With BBC Watchdog being a prime time show, our fraud prevention messages reached an audience of over 5.5 million for the live show and then a further 2.6 million people later in the week on the repeated programme. This is a crucial component of the strategy to prevent consumers falling victim to the courier scam, and further press work is planned throughout 2015.

Over the last year, at least £23.9m of losses can be attributed to vishing

<table>
<thead>
<tr>
<th></th>
<th>2013-14</th>
<th>2012-13</th>
</tr>
</thead>
<tbody>
<tr>
<td>£23.9m Up from</td>
<td>£7m</td>
<td></td>
</tr>
<tr>
<td>in the previous year</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
JOINING FORCES WITH PARTNERS, INCLUDING GOVERNMENT

FFA UK works, wherever possible, in a way which is complementary to initiatives led by other partners, including the government. There are common aspects to fraud affecting different sectors, and joining up activity can help deliver the step change we need in law enforcement. The following are examples of recent collaborative initiatives.

FFA UK, in conjunction with UK law enforcement, lobbied and worked with the telecommunications industry to put a stop to a technique fraudsters use to socially engineer customers over the telephone. The technique known as CLH (Caller Line Held) allowed criminals to stay connected to their victim over the telephone – unbeknownst to the victim who was under the impression he/she was speaking to the bank. Following on from this success, FFA UK is now working with the Telcos to look at addressing other techniques used by fraudsters. This includes preventing the misuse of Calling Line Identification (CLI) and SIM swapping.

Engaging with regulators and policy-makers
A major public affairs objective has been to achieve the best possible regulatory and public policy environment for fraud data-sharing. To this end, FFA UK is working with the Cabinet Office to deliver the legislative changes needed to facilitate more effective intelligence-sharing on known and suspected fraud. Minister for the Cabinet Office, Rt Hon Francis Maude MP, has praised the role of the financial services industry on the Counter Fraud Checking Service (CFCS) and underlined the government’s wish for continued co-operation looking forward. FFA UK has also worked alongside the BBA and supported the setting up of the Joint Money Laundering Intelligence Taskforce (JMLIT) – a twelve month pilot project to improve intelligence-sharing arrangements to support the fight against money laundering and other criminal activity.

Over this period, FFA UK has also informed and engaged a number of Opposition frontbench spokespeople, with a view to providing the same level of briefing support as that which we provide for incumbent Ministers.

FFA UK has also been exploring with officials at the Home Office and HM Treasury whether there is scope for government involvement in a national collaborative campaign on scams awareness.

“Over the past year we’ve seen an increase in counter fraud activity in both the public and private sectors. The threat is consistently evolving and we need to adapt to meet this challenge. This means improving cooperation across different sectors and improving the access to and exchange of information and analytical skills. We should also seek to support projects which help to develop analytical tools and extract the greatest value from the information gathered. Only then can we effectively work together to prevent fraud and reduce its opportunities to evolve.

I’m pleased to say that the Government is working closely with FFA UK in a range of projects to improve the use of data and resources; with the aim of reducing the cost of fraud within government, the banking sector, and to businesses across the UK as a whole.”

LESLEY HUME, EXECUTIVE DIRECTOR OF FRAUD, ERROR AND DEBT, CABINET OFFICE
FURTHER SERVICES AND ACTIVITY

Reference library
The industry landscape is constantly evolving, and keeping abreast of changes can be difficult for members acting alone. The FFA UK reference library makes available a collective store of information on new products and services that are likely to impact on the payments industry.

Indemnity Operational Working Group
This group was set up by FFA UK to provide a much-needed formal structure for managing and processing indemnities across the industry for the recovery of funds following a fraudulent transaction.

Members engage regularly and openly with one another as part of the case management process. The group has developed Best Practice Guidelines which articulate the key stages of the indemnity process, as well as the roles and obligations of all parties involved.

The Industry Hot Card File (IHCF)
The IHCF contains information on cards reported lost, stolen or compromised. When a participating retailer accepts a card payment as part of a normal transaction it is automatically checked against the file and the retailer is alerted if the details of the card match any of those on the system. Retailers who subscribe to this electronic file come from a wide variety of business sectors, including online outlets which have a time delay between taking an order and ensuring despatch. For these businesses, the IHCF is invaluable as a mechanism to provide a check on validity prior to fulfilment. An example of the application of the IHCF is at French motorway tollbooths to combat the use of stolen UK cards.

FFA UK website
The FFA UK website provides a wealth of advice for consumers and businesses on the simple steps they can take to protect themselves from becoming a victim of fraud. The site also provides guidance on fraud issues for law enforcement as well as a media centre which brings together facts, figures and latest news.

Visitors to the site can download and subscribe to publications developed by FFA UK – for example, the popular Fraud the Facts resource, which sets out in simple terms the current fraud trends and statistics, as well as the measures being taken by the industry to address fraud.

www.financialfraudaction.org.uk