Fighting Fraud:
Helping to keep customers safe

UK FINANCE

September 2018

TAKE FIVE TO STOP FRAUD

UK Finance

UK Finance represents nearly 300 of the leading firms providing finance, banking, markets and payments-related services in or from the UK. UK Finance has been created by combining most of the activities of the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and the UK Cards Association.

Our members are large and small, national and regional, domestic and international, corporate and mutual, retail and wholesale, physical and virtual, banks and non-banks. Our members' customers are individuals, corporates, charities, clubs, associations and government bodies, served domestically and cross-border. These customers access a wide range of financial and advisory products and services, essential to their day-to-day activities. The interests of our members' customers are at the heart of our work.

Contact: press@ukfinance.org.uk

www.ukfinance.org.uk

Table of Contents

Foreword

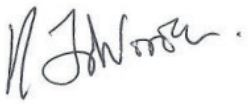
Recent high-profile data breaches have reminded us of the devastating impact fraud can have on victims, which is why it is imperative that we all work together to prevent it.

Criminals have become ever more inventive when it comes to fraud. In our latest fraud report, 'Fighting Fraud – helping to keep customers safe' we take a look at the latest tactics being adopted by fraudsters to try and steal consumers' money, from phishing to impersonation fraud to Authorised Push Payment (APP) fraud.

We also address some of the many ways in which banks are working together to tackle fraud and protect consumers, ranging from the Banking Protocol scheme, to the Take 5 campaign and to the use of biometric tools. Close cooperation between the banking and finance industry and law enforcement is also crucial in fighting economic crime.

Figures show that banks and card companies prevented more than £1.4 billion of unauthorised fraud in 2017 – equivalent to £2 in every £3 of attempted fraud. In the first half of 2018 banks and card companies prevented a further £705.7 million in fraud.

But there is more that needs to be done. Consumers and businesses are the first line of defence, which is why it is vital that we all understand the types of threat posed by fraudsters, and the ways in which we can all protect ourselves.



Katy Worobec
Managing Director, Economic Crime

A picture of fraud

Criminals have become ever more inventive in finding new ways to try and steal your money, through a variety of scams and frauds. We all know it's a threat and we all know it needs to be tackled, which is why the banking and finance industry is taking major steps and investing millions of pounds to protect consumers and businesses against fraud.

In 2017 nearly £1 billion was lost to fraudsters targeting consumers and businesses. Yet measures taken by banks and card companies helped to prevent £1.46 billion – equivalent to £2 in every £3 – of attempted fraud.

Banks prevented £1.46 bn fraud in 2017

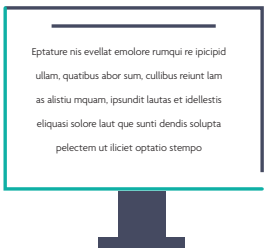
Equivalent to £2 in every £3 saved

Card fraud accounts for 80 per cent of all recorded fraud cases, or some 1.8 million cases in total. This is not surprising, given the volume of card transactions is growing rapidly.

Most of us will be aware of more simple forms of fraud, such as card fraud, when an individual's card or card details are stolen and used to make purchases on their account. Cards and PINs can be intercepted in the post, or simply stolen during distraction thefts, for example. Card fraud can also be a result of consumers having their personal data compromised while using unsecured or disreputable websites.

In recent years there has also been a steady increase in fraudsters using what are known as phishing, vishing and even 'smishing' scams to target consumers and get them to disclose personal and financial details.

This is when fraudsters send out emails, texts and even social media messages which are made to look as if they come from your bank or another organisation you might deal with regularly, such as utility companies or broadband providers asking you to provide your account details to resolve a 'problem'; or to download a document or programme which could infect your computer with malware; or to visit a fraudulent website – all with the aim of getting hold of your financial details and other useful information.



Phishing

Phishing is a technique used by criminals to try and gain funds or valuable personal financial information via email, by impersonating another person or legitimate organisation.

Vishing

Vishing is the term given to phonecalls or voice messages made by fraudsters with the aim of extracting personal financial information from the potential victim, or persuading them to transfer funds.

Smishing

Smishing is when fraudsters send out text messages with the aim of persuading consumers to hand over their personal information; or to download a virus or malware on to their mobile phone.

A data breach is when customers' personal and confidential information held by a company or organisation is leaked to an insecure or public environment, typically either because fraudsters have hacked into the firm's systems, or because of weaknesses or failings in a company's security procedures.

Data breaches from online businesses, retailers and utilities that hold consumers' personal data are also a major contributor to fraud and attempted fraud cases. There have been several high-profile cases in recent years, where data breaches by major organisations outside the financial sector have led to the personal details of millions of customers being exposed.

Criminals can use this stolen data to commit fraud directly, for example, card details are used to make unauthorised purchases online, or personal details are used to apply for credit cards, loans or other products. But more worryingly still, criminals use information gleaned through the data breaches to target individuals in impersonation and deception scams. Sometimes publicity around the data breach itself can add apparent authenticity to their approach.

Well-known major retailers, telecoms companies and many more have all suffered significant data breaches in recent years, which in turn have affected or compromised the details of millions of people.

All these types of fraud are known as 'unauthorised payments fraud', as the victim has had their financial information stolen or intercepted, and the fraudster uses that information to withdraw money from the card or bank account without the victim's approval.

Unauthorised fraud is the term used to cover areas such as card theft or cloning or fraud carried out as a result of a data breach which has left consumers' details exposed. In other words, the consumer did not 'approve' or ask for the payment to be made.

In the first half of 2018, losses due to unauthorised fraud on cards, remote banking and cheques fell by two percent to £358.0 million.

However, fraudsters are increasingly adopting 'social engineering' tactics to steal from consumers and businesses.

This is when fraudsters imitate banks or other trusted organisations that consumers have dealings with, to persuade them to hand over account details or often money. Criminals often use the 'dark web' to buy data enabling them to identify potential victims.

The fraudsters also take time to observe genuine communications from companies and imitate closely these methods and style of communications. They will know details that many believe only their bank or trusted provider could possibly know and use these tactics to convince customers to cooperate with them. They may also ask for details such as account security codes or transactions that a genuine company or bank would never ask for.

When consumers trust the fraudster in the belief they are dealing with a genuine approach or making a genuine payment to purchase goods or services, and as a result make a payment from their bank account to another bank account, this is known as authorised push payment (APP) fraud, also commonly referred to as an APP scam.

Authorised push payment (APP) is the term used to describe fraud carried out after criminals have managed to trick consumers into making a payment or transferring money to them in the belief that they are making a payment to a genuine person or organisation.

In the first half of 2018, £145.4 million was lost as a result of APP fraud.

This type of fraud includes a range of different scams. As well as fraudsters impersonating the bank or the police, APP also includes investment fraud – when people transfer funds in the belief it is a genuine investment opportunity; and romance scams, when people are duped by fraudsters into thinking they are in a relationship with them, often online and without ever meeting in person,

and to then agreeing to transfer money over to them. It could also include payment scams where fraudsters are purporting to sell something that does not exist or is fake (e.g concert or festival tickets or branded goods).

A major problem with APP fraud is that most cases don't look out of the ordinary or suspicious, so no alarm bells are triggered in the banks' fraud detection and monitoring systems. The payment is coming from the customer and from their usual laptop or tablet, the payment size is often not unusual, and, most importantly, the customer has authorised the payment. The characteristics of the payment look normal.

The industry is continuing to develop new analytics and profiling tools to identify potential APP fraud payments being received by beneficiary accounts – the accounts to which funds are being transferred. However, even here there are difficulties. Most accounts are set up perfectly legitimately and pass all of the legal and regulatory money laundering checks carried out by banks.

In cases of fraud the account may operate normally for years and then the accountholder either has their account taken over, is persuaded to sell the account, or becomes what is called a 'money mule'. This is almost impossible to spot before it goes bad.

A money mule is the term used to describe someone who is recruited by criminal gangs, sometimes unwittingly, to help with the transfers of money between different bank accounts.

A key way to tackle this issue is by more rapid sharing of information between banks about suspicious accounts – something which the industry is currently hampered from doing by money laundering regulations and general data protection regulations.

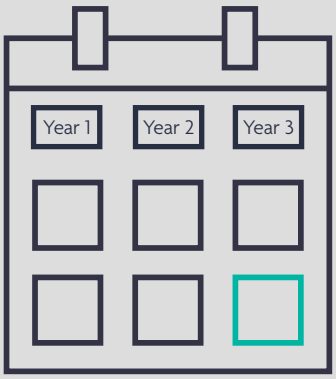
This is why fraudsters have increasingly focused their efforts on so-called money mule accounts.

In many cases fraudsters will post apparently legitimate adverts offering financial incentives to those prepared to transfer money on their behalf.

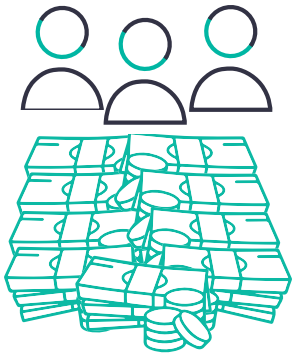
Criminals have increasingly targeted students, paying them money to allow their bank account to be used to transfer funds. In other cases, overseas students finishing their studies in the UK are being paid to hand over their bank accounts and details, if they are leaving the country.

In many cases people may not realise allowing their accounts to be used in this way is illegal and that they are facilitating money laundering, which could lead to a jail sentence for anyone involved.

Industry statistics show that in cases where an account has either been taken over or sold, it has, on average, been open for three years before fraud begins to be committed.



Who is behind fraud?



Fraud is clearly not a victimless crime. Even if victims are refunded or the fraud is detected and prevented, it can still cause immense distress and the consequences can be enduring.

But it is not only the victims of fraud who suffer. Fraud is being driven by organised crime gangs who are ruthless and make millions of pounds, which in turn funds the illegal drug trade, terrorism and human trafficking.

As Tony Blake, of the Dedicated Card and Payment Crime Unit (DCPCU) says: "This is not a case of teenagers sitting in their bedrooms trying to fool people or companies into handing over money.

"These criminal gangs are run as businesses. They can make millions of pounds from fraud and they invest in their business, for example, they will have researchers who are paid to investigate the way banks and companies communicate, to find the best way to con people by impersonating legitimate organisations.

"In particular social engineering, which is on the rise, is a clever manipulation of the natural human tendency to trust, good fraudsters prey on this trust which is why we must always be on our guard."

Social engineering is a clever manipulation of the natural human tendency to trust.

Criminals are also using 'money mules' to launder money from the proceeds of crime. Mules will usually be unaware of where the money comes from – fraud, scams and other serious crimes – or where it goes.

Worryingly, police are warning that the fastest growing group of people targeted to be money mules now is 11 – 18-year olds. In some cases, youngsters are being groomed by people they know through sports or leisure clubs, or by gangs.

Parents are being asked to be vigilant and help to educate their children to prevent them falling into this type of fraud, and to identify possible signs that they have been groomed by fraudsters in this way – for example, if they suddenly have lots of money or expensive goods that have no obvious source of funding.

People are not always who they say they are.

What is the industry doing to prevent fraud?

Dedicated Card and Payment Crime Unit (DCPCU)

Individual financial institutions are continuously investing in new ways to detect fraud and protect their customers. Through UK Finance, they also support a number of industry-wide initiatives.

A key element in the fight against fraud is the Dedicated Card and Payment Crime Unit (DCPCU), which was established in 2002. This specialist police unit is funded entirely by the industry and consists of officers from the Metropolitan Police and City of London Police, working together with UK Finance staff.

The DCPCU targets organised criminal groups responsible for card and payment fraud and takes referrals from banks and card companies, as well as generating cases from intelligence they source themselves.

In the first half of 2018 alone the DCPCU has prevented £25 million of fraud, made 84 arrests and seen 26 fraudsters convicted. Since being set up in 2002 it has produced estimated savings of more than £540 million.

The DCPCU led a joint operation between Europol and 28 police forces in June, which led to close to a hundred arrests for remote purchase or card-not-present fraud.

The DCPCU has three key priorities to tackle –

- Social engineering – including APP scams
- Card-not-present (CNP) fraud
- Insider fraud (working closely with the industry, the DCPCU makes at least one arrest a week)

Fraud losses on UK-issued cards totalled **£566 million** in 2017

from £618 million in 2016. **8%**

This was the first decrease reported in six years.

Overall card fraud losses fell from

8.3p per £100 spent in 2016

7.0p per £100 in 2017

Total spending

£755 billion in 2017

The Fraud Intelligence Sharing System

The Fraud Intelligence Sharing System is an industry-wide database designed to support card providers and retail banks in the fight against fraud. Users submit details of frauds to the system, which then identifies linked cases and patterns in fraud and enables protections to be put in place. Card providers and banks using the system collectively saved £12 million in 2017, our figures show.

The system means that the collated fraud data and intelligence and the insights can be shared with other agencies, including police, the National Crime Agency and the National Fraud Intelligence Bureau. The NFIB informs law enforcement activity in the UK, ensuring the police have greater insight with which to protect consumers and businesses.

Figures from the Office for National Statistics show that in the 12 months to June 2017, the industry shared intelligence on over 87,000 fraud offences with the NFIB, or directly with law enforcement.

The ability to share valuable information also allows the industry to set up strategic partnerships with other (non-financial) sectors to fight financial fraud, including Royal Mail.

Financial Fraud Bureau (FFB)

Established in 2010, the Financial Fraud Bureau leads the payments industry's collective initiatives on fraud intelligence and data sharing. Its key roles are:

- Disseminating intelligence directly from, and to banks, card schemes, card issuers and acquirers, and a wide number of stakeholders, including police forces and other law enforcement organisations
- Gathering, collating and analysing the intelligence that informs the Industry Strategic Threat Management Process
- Being the single point of contact for companies suffering data breaches to ensure compromised account information can be speedily, safely and securely repatriated to the banks
- Coordinating intelligence alerts from the payments industry and other key players ensuring that alerts are issued.

Through the FFB, the industry can be alerted immediately of any known compromise of bank or card data through a series of designated Single Points of Contact (SPOCs). The FFB works with the 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.

Public-Private Partnerships

The Joint Fraud Taskforce was set up in 2016 as a partnership between the Home Office, banks and police, with the aim of tackling fraud, in particular, issues considered too difficult for a single organisation or sector to manage alone.

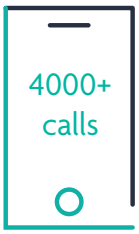
Similarly, the Joint Money Laundering Intelligence Taskforce is a partnership between banks and the National Crime Agency (NCA), set up to tackle money laundering. Working within the NCA allows the banks to share information in a way that would not be possible otherwise because of money laundering regulations.

Banking Protocol scheme

In early 2017 the industry launched the Banking Protocol scheme, which enables bank branch staff to immediately alert police if they believe a customer is at risk of fraud and financial loss.

The system is now operational in every police force area and in the first six months of this year prevented £14.6 million in fraud. Since launch nearly £28 million of attempted fraud has been prevented, with around £3 million a month on average now being stopped. More than 4,000 emergency calls have been made so far, and close to 230 criminals have been arrested.

As well as protecting customers from becoming the victim of fraudsters and suffering financial losses, the scheme has also helped to prevent the distress caused to those who are successfully targeted, as well as reduce the likelihood of them becoming a victim of fraud in the future.



Case Study

Activating Banking Protocol

An elderly customer called at a branch of RBS, asking to transfer funds to cover a cheque she was planning to issue. The branch asked some more questions and learned that the payment was for £9,000 for loft insulation – an unusually high sum for the customer. It transpired that the customer had had a trader call at her home to offer to carry out the work for her, and she had been asked to make the payment upfront. Suspicions were raised so the branch decided to activate the police Banking Protocol immediately. The police attended the branch and, given the customer's age, also accompanied her home to speak to the trader. As a result, the loss of the customer's £9,000 – and potentially much more – was prevented.

Case Study

The Protocol protects

Staff at a Co-Op bank branch in Nottingham intervened when they were suspicious that an 88-year old customer was being duped by a fraudster claiming to be a financial advisor. The staff decided to use the Banking Protocol scheme to alert police. As a result, the staff in the branch were able to stop the customer from becoming a victim and potentially losing £92,000.

Technology to fight fraud

Banks are sharing data to help detect fraud at an early stage.

The banking industry is also proactively using technology in the fight against fraud. One example is the use of a system – described as a global digital identity tool – which has been adopted by a number of leading banks to help identify and prevent potential fraud.

The system works by analysing billions of real-time transactions across many countries including the UK, coupled with additional data including device, geographical, behavioural and threat intelligence input, to identify suspicious transactions and potential criminal activity.

The technology is particularly powerful when it comes to identifying money mule accounts, where banks can analyse data anomalies to reveal webs of linked accounts generated by mule activity.

The system also uses historical activity to build a picture of the customer's behaviour, in terms of the timing and types of transactions, which is then matched against new transactions. This enables unusual and potentially fraudulent activity to be identified and flagged up.

Some banks are using technology which allows them to identify the different sound tone that every phone has and the environment that they are in. If someone is calling from an environment which is not their usual one, this can be picked up, and investigated further to detect if fraud is being attempted.

Banks are using biometric tools to identify fraud.

Banks are also increasingly looking at 'behavioural biometrics' tools to identify potential cases of fraud and prevent them where possible. Some banks have adopted software that monitors the ways in which consumers type and swipe on their devices or how they hold their device in terms of grip, when logged into banking apps.

If this 'behaviour' changes then the software will flag up potentially suspicious activity and could prompt a call from the bank. Use of this technology has helped to prevent tens of thousands of pounds of fraud going through. Other banks use technology to prevent products and services being accessed by devices that have been linked to fraud.

Many banks now employ teams of dedicated investigators to identify and manage out money mules. These investigators will use leading technology to detect customers, with reference to their transactional profile and behaviour, network and device.

Banks can identify the sound tones of individual phones.

Banks are now increasingly sharing data to ensure that this activity is detected at an early opportunity, accounts are blocked, and where funds are available, they can be frozen.

Working together

There are a wide variety of ways in which banks, card issuers and the industry generally are looking to help prevent fraud and protect consumers and businesses. A key tool is increasing collaboration with other – often non-financial – sectors, working together to identify and tackle fraud.

One such example is the telecoms sector, which the industry has been working with to prevent cases of vishing, in particular. Banks have worked with telecom companies and the regulator Ofcom so that phone lines will shut down within a matter of seconds. This initiative was taken in response to fraudsters calling potential victims and then inviting them to call back in order to 'prove' the call was genuine. Previously fraudsters were able to keep the phone line open for longer, without the knowledge of the victim who thought they were calling a new number.

The industry has also worked with Royal Mail, through the Fraud Intelligence Sharing System (FISS), sharing data on geographical fraud 'hotspots' and enabling Royal Mail to investigate these areas where there is a high or higher risk of fraud than elsewhere, and take steps to protect its customers.

Education and training

Many banks have fraud warning videos available in branches and on their websites, providing customers with information on common and emerging frauds, along with advice as to how they can protect themselves.

A number of banks are holding fraud seminars for staff, individual and business customers, at which details of the latest scams and ways in which customers can protect themselves against fraud are top of the agenda. These include face to face training for small and medium-sized firms, who are particularly being targeted with cases of invoice fraud.

Customers are also being advised about the risks of social media and the need for people to be aware of the data they may be making publicly available, sometimes without realising. There is information about the free tools that can be used by consumers and businesses to protect themselves, or tools such as 'Have I Been Pwned?' which lets people know if their email has been compromised.

All banks are working towards – and a number already have in place – introducing 24-hour staff response schemes, to help deal with and process APP scam complaints.

Coming soon...

This autumn the Banking Protocol will be extended to telephone transactions under a three-month pilot scheme. Initially two banks are taking part, along with Sussex police, with the plan to roll this out further if successful.

Under the scheme, if the banks receive a phone call from a customer that seems odd or unusual, for example, if its a request for an unusually high transaction, they will ask the customer if everything is ok. If the customer says yes, they will carry on – but ask the customer to go to a branch to complete the transaction.

In cases of 'vulnerable' customers, the bank branch will work with local police to assess whether the transaction is fraudulent or genuine, which could lead to the transaction being temporarily blocked if necessary to protect the customer.

There are also plans to look at extending the Banking Protocol scheme to get supermarkets on board. It comes as a growing number of Bureaux de Change and money transfer outlets in supermarkets are reporting potentially suspicious transactions.

In November the Money Mules campaign will focus on helping to protect schoolchildren, in particular those 11-18 years of age, who are increasingly being targeted by fraudsters. Local police will be working with schools in their area, with schools sending out a UK Finance and local police branded letter warning parents to make sure their children do not become money mules and of the risks. The leaflet will advise parents who think their child may be being groomed to contact Action Fraud.

In 2019 banks and building societies will be able to introduce a 'Confirmation of payee' service. Currently, electronic payments are addressed using just the sort code and account number – confirmation of payee will offer a way to check the name of the account holder you are paying before you confirm the payment.

Confirmation of payee should prevent payments being sent to the wrong account due to unintentional errors, and it will make it harder for fraudsters to trick someone into sending money by posing as a legitimate person or organisation.

Where are we now, better or worse?

Banks have invested millions in tightening up their systems and these steps mean it is now harder for fraudsters to defeat the banks' security measures.

Criminals have increasingly turned their focus onto consumers instead, as well as other sectors or organisations where there may be gaps in security. Now, the vast majority of fraud involves criminals targeting customers or third-party organisations for data and security information, or to transfer money. This means customers are the first line of defence.

While losses from unauthorised fraud are falling, the amount of attempted fraud is rising. Meanwhile, losses from authorised fraud have risen sharply, with criminals increasingly targeting consumers and businesses, in particular the elderly and vulnerable.

Banks and card companies prevented £2 out of every £3 of attempted fraud – equivalent to £1.46 billion in 2017 alone. While fraud is a very real threat, consumers should feel reassured by the security measures that are now in place to prevent and detect fraud and the continued push by industry to develop further protections.

> As it has become harder for the fraudsters to get money from the banks, so they have shifted to consumers, for the low-hanging fruit.

Why it's important we all pull together to fight fraud

Developments in technology, greater awareness of fraud techniques and closer monitoring are helping banks and financial services organisations to identify and prevent the majority of attempted fraud.

But fraudsters – organised criminal gangs – are not giving up. For them fraud is a business and one they carry out day in day out. They are always a step ahead, socially engineering customer behaviours and looking for vulnerabilities, wherever they may be.

Ensuring a high level of awareness among consumers as to the risks and threats posed by fraudsters and how they can protect themselves is vital. The question should be 'How do we prevent fraud before it has happened?', rather than simply reacting after the event.

The national fraud awareness campaign Take 5 (led and funded by UK Finance and its members and backed by government) encourages consumers to 'stop, think and take five' before going ahead with a financial transaction, in order to reassure themselves that it is not an attempt by fraudsters to steal their money or details. So far more than £2.3 million has been spent in trying to raise awareness of fraud to help consumers and businesses protect themselves. The third stage of the campaign will launch early next year.

As industry strives to continually improve its response to fraud, it is important that other sectors play their part by securing customers' data. Equally, consumers and businesses need to take steps to protect themselves against these insidious crimes.

Information, guidance and tips about how consumers and businesses can protect themselves is available in a wide range of places and formats, including on the Take 5 – To Stop Fraud website.

But the key messages are worth remembering:

- A genuine bank or organisation will never contact you out of the blue to ask for your PIN, password or to move money to another account.
- Never click on a link in an unexpected email or text – you could be giving access to your personal and financial details.
- Always question uninvited approaches in case it is a scam. Instead, contact the company directly using a known email or phone number.
- Don't assume an email or phone call is authentic – just because someone knows your basic details (name and address, or mother's maiden name) it doesn't mean they are genuine.
- Don't be rushed into making a decision or financial transaction on the spot – a genuine bank or trusted organisation would never do this.
- Listen to your instincts – if something feels wrong then it generally is.
- Take 5 – take time to think about whether this is genuine or if it could be an attempted fraud.

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