HOUSE OF COMMONS LIBRARY

BRIEFING PAPER

Number 8545, 22 July 2019

Banking fraud

By Oliver Bennett MBE & Jennifer Brown
Jennifer Brown

Contents:

Contents

Summary

Criminals successfully stole £1.2 billion from individuals through banking fraud and scams in 2018.[1] Businesses and the public sector are estimated to lose around £5.9 billion per year.[2]

Most fraud targeted at individuals is conducted via **unauthorised** payments from payment cards, remote banking and cheques. Victims of this type of fraud can often get the money back from their bank, depending on the circumstances of the loss.

However, a significant amount of fraud in 2018 was also via **authorised** payments. This is when the victim is tricked into transferring the money to the criminal.

In these cases, victims were much less likely to recover their losses. In 2018, only 23.3% of losses from authorised payments (£82.6m) was returned to victims. This was either by a full or partial refund directly from the bank or when the funds were recovered from the recipient bank.

A code of practice introduced in May 2019 gave a commitment, from all firms who sign up to it, to reimburse victims of authorised payment scams in any scenario where the customer has met minimum standards expected of them under the code.[3]

Police response

The City of London Police leads the police response to fraud. They are home to two national units (Action Fraud and National Fraud Intelligence Bureau) where fraud cases are reported and analysed. If these units believe there is enough evidence, they will allocate cases to a local police force for investigation.

The police response to fraud has come under much criticism. There are concerns that a high number of cases do not reach the threshold for investigation and that those that do rarely result in offenders being bought to justice. Various stakeholders have called for better co-ordination across the police to improve service to victims and the quality of investigations.

Advice for victims of fraud

Victims of banking scams should consult the Action Fraud website, which:

- allows victims to report fraud to the police;
- describes what victims need to do should they become a victim of this crime;
- describes the different types of fraud;

---

[1] "FRAUD THE FACTS 2019: The definitive overview of payment industry fraud", *UK Finance* [online], 21 March 2019 [accessed 8 April 2019]

[2] Serious and Organised Crime Strategy, Cm 9718, November 2018

[3] "APP Scams Steering Group Agrees Voluntary Code", *APP SCAMS STEERING GROUP,* 28 February 2019 [accessed 8 April 2019]

- gives practical advice to individuals and businesses on how to protect themselves.

The 'Take Five' website, which is a national awareness campaign led by industry and Government also offers advice to victimshttps://takefive-stopfraud.org.uk/advice/.

If a bank or service provider refuses to reimburse a victim of a bank scam, the Financial Ombudsman Service can investigate whether the bank took the appropriate decision.

1. Banking scams

1.1 Types of scam

Scams can broadly fit into two categories: authorised and unauthorised.

Unauthorised fraud is where the account holder does not provide authorisation for the payment to proceed and the transaction is carried out by a third party. Fraudsters obtain banking details to do this, such as by cloning cards, hacking accounts or persuading victims to give them their details.

Authorised fraud involves the genuine customer being tricked into paying money into another account that is controlled by a criminal. This is also known as Authorised Push Payment (APP) fraud.[4]

Criminals use a range of communication methods to deceive their victims, including phone calls and emails. UK Finance reported that criminals are also "increasingly using social media sites to entice victims with posts advertising items for sale and investments, both of which are fake".

It has been reported that the use of 'social engineering' techniques was a major contributor to both authorised and unauthorised fraud losses in 2018.

These are techniques that criminals use to groom and manipulate people into transferring them money or divulging their personal and financial details. Such techniques include impersonating an authority figure, developing a friendly relationship with the victim and creating a sense of urgency to encourage poor decision-making.

One such scam involves criminals, posing as a representative of a government department, contacting victims by telephone to tell them they are eligible for a refund for poor broadband services. Victims are persuaded to hand over their banking information to receive their 'refund'. The criminals then use this information to withdraw money from the victim's account.[5]

A detailed and lengthy A-Z list of scams can be found on the Action Fraud website.

1.2 The scale of the problem

UK Finance states that criminals successfully stole £1.2 billion through banking fraud and scams in 2018.[6]

Most of this was through unauthorised payments across payment cards, remote banking and cheques:

---

[4] "APP Scams Steering Group Agrees Voluntary Code", *APP SCAMS STEERING GROUP,* 28 February 2019 [accessed 8 April 2019]

[5] "FRAUD THE FACTS 2019: The definitive overview of payment industry fraud", *UK Finance* [online], 21 March 2019 [accessed 8 April 2019]

[6] "FRAUD THE FACTS 2019: The definitive overview of payment industry fraud", *UK Finance* [online], 21 March 2019 [accessed 8 April 2019]

- losses totalled £844.8 million, an increase of 16 per cent compared to 2017.
- Banks and card companies detected and prevented £1.66 billion of unauthorised fraud losses. That equated to around 67%, or £2 out of every £3, of losses that were detected and prevented by firms.

However, losses due to authorised payments were also significant. Victims of this type of fraud lost significant sums:

- Overall losses were £354.3 million. This was split between personal (£228.4 million) and nonpersonal or business (£126 million).
- 23.3% of losses (£82.6m) were returned to victims. This was either by a full or partial refund directly from the bank or where funds were recovered from the recipient bank.
- There were 84,624 cases relating to a total of 83,864 victims. Of this total, 78,215 cases were on personal accounts and 6,409 cases were on non-personal accounts.

More information about the scale of different types of scam can be found in Fraud the Facts 2019, by UK Finance.

2. Police response

Individual police forces are responsible for investigating fraud cases in their police force area, including banking scams. There is currently no national policing strategy for tackling fraud. However, there is some coordination between law enforcement agencies on fraud. Most notably, there is a coordinated system for reporting fraud to the police which is led by the City of London Police Force.

Reporting fraud

All cases of fraud should be reported to the City of London Police. The City of London Police acts as the 'lead police force' for fraud and economic crime.[7] It is home to two national units, Action Fraud and the National Fraud Intelligence Bureau (NFIB), which record and analyse fraud cases. These units assign fraud cases for investigation to the relevant police forces.

City of London Police receives an annual grant from the Home Office to run Action Fraud and the NFIB.[8] In 2017/18 this grant was worth £8 million.[9]

There are limited circumstances in which a police force can record a fraud case locally and launch an investigation without analysis from City of London Police. Normally, for a force to do so, the case should be 'local' and officers should be able to easily identify suspects.[10] Police forces should still report cases they have recorded locally to the City of London Police.[11]

Action Fraud

Action Fraud is the UK's 'reporting centre' for fraud cases. Victims of fraud (both individuals and businesses) can report their case directly to Action Fraud online or via the telephone. Local police forces can also pass fraud reports to Action Fraud.

Staff at Action Fraud log fraud reports and provide victims with a crime reference number. These individual crime reports are then passed to the NFIB to be analysed.[12]

Action Fraud's 'contact centre' is managed, under contract, by a private company called Concentrix. Previously, the contact had been held by the not-for-profit organisation '*Broadcasting Support Services*' but this organisation went into administration in 2015.[13]

---

7 City of London Police, National Policing Lead For Economic Crime Annual Review 2016 – 2017, undated
8 HMCFRS, Fraud: Time to Choose: An inspection of the police response to fraud, April 2019, p8
9 PQ168183: Cybercrime, answered on 10 September 2018
10 Home Office, Counting Rules for Recorded Crime: Fraud, April 2019
11 Ibid
12 Action Fraud, What is Action Fraud? [last accessed 22 July 2019]
13 House of Commons Home Affairs Committee, Policing for the future: Tenth Report of Session 2017–19, October 2018, paragraph 47

National Fraud Intelligence Bureau

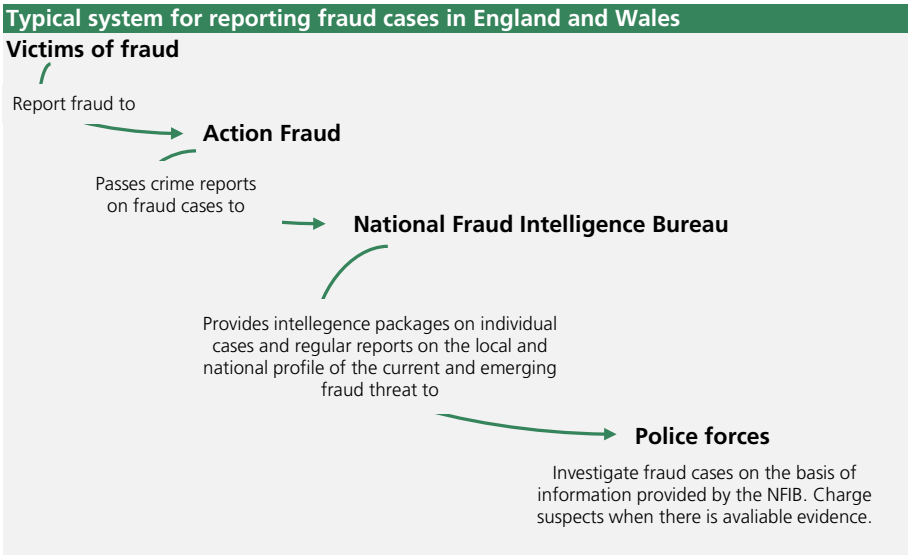
The NFIB analyse crime reports passed to them by Action Fraud. If they think that there is a realistic prospect of identifying an offender and securing a conviction they will allocate the case to the relevant police force for investigation.[14] If not, they will log the case on NFIB systems and inform the victim (through Action Fraud) that no further action will be taken.[15] Frequently asked questions about this system can be found in the following section of this briefing paper.

The NFIB provide a 'intelligence package' to the local police forces on the cases it allocates to them. Police forces use this information to assist their investigations.

Police forces are operationally independent and make their own decisions about what cases to investigate. Sometimes individual forces will determine that there is not enough evidence to launch an investigation even when a case has been allocated to them by the NFIB.

The NFIB also provides police forces with regular updates on the fraud threat level including up-to-date victim profiles.[16] To do so they combine information from individual fraud reports with data provided to them by the finance industry.

The NFIB stores all the information it gathers on fraud in a centralised database known as 'Know Fraud'.[17] This system prioritises which cases will be reviewed by NFIB staff.[18]



Investigating fraud

Local police forces have operational discretion and can choose whether to launch an investigation into a fraud case or not. However, there are Home Office Counting Rules which determine how they should handle reports of fraud that come directly to them. These rules specify the

14 Ibid, paragraph 9.10
15 HMICFRS, Real lives, real crime: A study of digital crime and policing, December 2015, paragraph 9.13
16 Ibid, paragraph 9.7
17 Ibid, paragraph 9.9
18 Home Office, The scale and drivers of attrition in reported fraud and cyber-crime: Research Report 97, June 2018, p11

limited types of cases they can record locally. As discussed above, most fraud reports should be channelled through Action Fraud and the NFIB.

The College of Policing (the professional body for policing in England and Wales) has published official guidance on investigating fraud but they have not made this guidance publicly available.[19]

Individual police forces handle fraud cases differently. Some have dedicated teams which investigate fraud, others allocate fraud cases to teams that specialise more widely in economic crime. Some forces have no specialist resource for investigating fraud at all.[20]

2.1 Concerns about police response to fraud

There have been longstanding concerns that the police response to fraud is inadequate. Data on police fraud investigations is unreliable but there is evidence that a high number of reported cases fail to reach the threshold for investigation.[21] There are also concerns that cases that do reach investigation have low success rates. Estimates suggest that as little as 3% of cases reported to Action Fraud result in charges or summons being brought against an offender.[22]

The Home Affairs Select Committee concluded in its 2018 report on Policing for the Future that the "police response to fraud is in desperate need of a fundamental overhaul".[23] The inspectorate of police forces has said that some practices in police forces are "intolerable" and have called on the Government and police leaders to work together to ensure that "there is a clearer strategy, less variation in service between forces and better communication with the public."[24]

Broadly, the concerns with the police response to fraud are:

- The current system is fragmented and inadequate for tackling a crime which crosses police force boundaries and borders.
- Action Fraud and the NFIB provide a poor service to victims of fraud and police forces.
- Police forces do not prioritise fraud. The lack of resources dedicated to fraud means that many forces have failed to develop the specialist skills needed to investigate it. This has resulted in a large number of poor-quality fraud investigations.

19 College of Policing, Investigation: Investigating fraud, January 2019 [last accessed 22 July 2019]
20 HMCFRS, Fraud: Time to Choose: An inspection of the police response to fraud, April 2019, p11-12
21 Home Office, The scale and drivers of attrition in reported fraud and cyber-crime: Research Report 97, June 2018
22 House of Commons Home Affairs Committee, Policing for the future: Tenth Report of Session 2017–19, October 2018, paragraph 57
23 House of Commons Home Affairs Committee, Policing for the future: Tenth Report of Session 2017–19, October 2018, paragraph 66
24 HMCFRS, Fraud: Time to Choose: An inspection of the police response to fraud, April 2019, p5

Co-ordinating the police response to fraud

There is currently no 'national strategy' for policing fraud but there is some co-operation between law enforcement partners, government and industry on tackling the crime:

- As part of its Serious and Organised Crime Strategy the Government have convened the Economic Crime Strategic Board with responsibility for steering the response to serious and organised fraud and established a National Economic Crime Centre in the National Crime Agency responsible for co-ordinating the UKs response to economic crime.
- The Government established a Joint Fraud Task Force.
- Police leaders have published ad-hoc guidance and other policy documents.

The inspectorate of police forces, the Home Affairs Select Committee and other stakeholders have been critical of these co-ordination efforts. All agree that more needs to be done to standardise services. However, there is some disagreement about whether investigations of fraud should be investigated locally or not.

In its 2019 thematic inspection of the police response to fraud the inspectorate concluded that the "current model of local investigations supported by national functions is the right one".[25] However, they did recommend that the National Police Chiefs Council (a co-ordinating body for UK police forces) should set a policing strategy for fraud by March 2020.[26] The inspectorate hopes that a national strategy will improve coordination between forces and set clear roles and responsibilities for local, regional and national actors.

The Home Affairs Select Committee recommended in their 2018 report Policing for the Future that the current model of local investigations be replaced. They called on the Government to

> …implement a 'hub and spoke' structure for fraud investigation and victim support, with all investigations undertaken at a national or regional level.[27]

The Police Foundation (a policing policy thinktank) agree with the Home Affairs Select Committee that fraud investigations should not be undertaken by local forces. They have argued that

> Police forces and local PCCs should focus on supporting vulnerable victims and coordinating local prevention work, while fraud investigations should be carried out by dedicated regional teams working within an accountable national network.[28]

Co-ordination on serious and organised fraud

The Government identified fraud as a key form of serious and organised crime in their latest Serious and Organised Crime Strategy (published November 2018). As part of the strategy the Government has set up two new bodies with responsibility for 'economic crime' including

---

25 Ibid, p4
26 Ibid, recommendations 5
27 House of Commons Home Affairs Committee, Policing for the future: Tenth Report of Session 2017–19, October 2018, paragraph 66
28 The Police Foundation, More than just a number: Improving the police response to victims of fraud, December 2018, p81

serious and organised fraud (i.e. fraud that is conducted by organised crime groups).

In December 2017 the Government announced that it would invest £4.6 million to establish the National Economic Crime Centre (NECC) within the National Crime Agency. The NECC co-ordinates law enforcement's response to economic crime.

In January 2019 the Home Office established the Economic Crime Strategic Board. This board is chaired jointly by the Home Secretary and the Chancellor of the Exchequer and includes representatives from the finance industry and the National Crime Agency. It is responsible for setting priorities and directing resources to tackle the economic crime threat set out in the Serious and Organised Crime Strategy. It will also scrutinise how well industry and law enforcement tackle economic crime.

The inspectorate has recommended that the roles and responsibilities of the NECC and how this relates to the responsibilities of the City of London Police (as the lead force for economic crime) should be clearly defined to avoid duplication.[29] They also recommended that the Economic Crime Strategic Board expand its remit to include fraud in its totality and not only fraud that is conducted by organised crime groups.[30]

Joint Fraud Taskforce

The Government established a Joint Fraud Taskforce (JFT) in February 2016.[31] Improving the law enforcement response to fraud is one its 'five areas of focus'. To date, JFT's progress on improving law enforcement response to fraud has been limited. In January 2018 a paper by JFT on best practice for investigating fraud was agreed by the NPCC.[32] However, this paper has not been made public.

The Home Affairs Select Committee have been highly critical of JFT. They say it has "little to show for two and half years of work" and that they "are not sure what the point of it is, in practice".[33] The National Audit Office (NAO) have also been critical. They concluded that the Taskforce has "no clear success measures for its initiatives" and that it lacked transparency about its work.[34]

The last published meeting minutes for JFT's management board are from June 2018.[35] In this meeting the JFT discussed an 'independent review' of its work which found that "aspects of the Taskforce needed strengthening". The management board agreed that a new threat

29 HMCFRS, Fraud: Time to Choose: An inspection of the police response to fraud, April 2019, recommendation 5
30 Ibid, recommendation 3
31 Joint Fraud Taskforce, The Joint Fraud Taskforce newsletter: Edition 1, January 2017
32 NPCC, Chief Constables' Council Minutes Wednesday 24 – Thursday 25 January 2018, paragraph 4.3.17
33 House of Commons Home Affairs Committee, Policing for the future: Tenth Report of Session 2017–19, October 2018, paragraph 71
34 NAO, Online fraud, June 2017, paragraph 2.14
35 Joint Fraud Taskforce, Management board minutes of meeting held 20 June 2018, June 2018

assessment of fraud would be undertaken and that a new programme plan for JFT would be developed based on it.[36]

In March 2019, the Government said that JFT will

> …publish its plans, based on the review's findings, together with its activity, reports on progress and measures of success, once its objectives, priority projects and resourcing have been reset.[37]

Police leaders

Senior leaders in the police service have published ad-hoc guidance and policy documents relating to fraud. In January 2017 the NPCC agreed a 'roles and responsibilities grid' for fraud which sets out expected responses at force, regional and national levels.[38] In 2015 the City of London Police published a Draft National Policing Fraud Strategy and a Draft National Fraud Protect Strategy. However, the inspectorate has found that individual forces are not making good enough use of these documents and that awareness of them across the police service is low.[39]

Action Fraud and NFIB

The performance of Action Fraud and the NFIB has been the subject of much criticism. They have been accused of providing poor communications to victims of fraud and police forces and for taking too long to handle requests. The Home Affairs Select Committee has gone as far as to claim that Action Fraud has "irretrievably lost the confidence of the public".[40]

In its 2019 inspection of the police response to fraud the inspectorate of police forces found:

- 37% of calls to Action Fraud in the year to March 2018 were unanswered. Of the calls that were answered the average caller waited on hold for 16 minutes. [41]
- Delays of up to three months in NFIB staff carrying out case reviews on crime reports passed to them by Action Fraud.[42]
- Instances where the NFIB took up to four weeks to review a force request for a case to be reallocated.[43]

The inspectorate was also critical of NFIB 'products' to police forces. They found that intelligence packages on allocated fraud cases were "not easy to read or interpret" and "would be difficult to use for investigators who were either, not trained to deal with fraud or who

---

36 Ibid
37 Home Office, The Government response to the tenth report from the Home Affairs Select Committee Session 2017-19 HC515: Policing for the future, March 2019, paragraph 30
38 HMCFRS, Fraud: Time to Choose: An inspection of the police response to fraud, April 2019, p9
39 Ibid, p40 & 42
40 House of Commons Home Affairs Committee, Policing for the future: Tenth Report of Session 2017–19, October 2018, paragraph 50
41 HMCFRS, Fraud: Time to Choose: An inspection of the police response to fraud, April 2019, p12
42 Ibid, p15
43 Ibid

were not regularly investigating it."[44] They also found that regular reports on the fraud threat level were not being consistently used by forces because police staff found them unhelpful.[45]

The inspectorate has recommended that the Home Office set out clearly terms for its funding agreement with the City of London Police to run Action Fraud and the NFIB. They say these terms should include accountability and governance processes and an assessment of the City of London Police's performance.[46]

The Government has insisted that "victims are receiving a much-improved service" from Action Fraud thanks to a new online reporting service.[47] The Government invested £5.5million in a new online reporting system for Action Fraud that went live in 2018.[48]

Quality of investigations

The 2019 inspection of the police response to fraud found that there are "significant problems with the way fraud is currently investigated, including numerous examples of inefficient and ineffective processes."[49] The inspectorate found a number of specific problems with current police practice. These include:

- Investigators lack the information they need to conduct their investigations. This is largely down to poor information sharing from the NFIB.
- Too many investigations are undertaken by officers who lack the appropriate skills and knowledge.
- Local forces do not always take advantage of regional and national hubs of expertise (such as the City of London Police) to aid their investigations.[50]

The inspectorate recommended that the NPCC and the College of Policing (the professional standards body for policing in England and Wales) work together to identify, evaluate and disseminate best practice advice on responding to fraud across the police service.[51]

---

44 Ibid, p16
45 Ibid, p9
46 Ibid, recommendation 4
47 Home Office, The Government response to the tenth report from the Home Affairs Select Committee Session 2017-19 HC515: Policing for the future, March 2019, paragraph 26
48 HM Treasury, Treasury Minutes Government response to the Committee of Public Accounts on the Fourth to the Eleventh reports from Session 2017-19, paragraph 5.5
49 HMCFRS, Fraud: Time to Choose: An inspection of the police response to fraud, April 2019, p65
50 HMCFRS, Fraud: Time to Choose: An inspection of the police response to fraud, April 2019, pages 65-80
51 Ibid, recommendation 6

3. Industry and Government action

The banking industry has a broad regulatory requirement to provide a safe banking environment. UK Finance, which represents the banking and finance industry, set out the actions the industry is taking to address banking scams:

- **Investing in advanced security systems** to protect customers, including real-time transaction analysis, behavioural biometrics on devices and technology to identify the different sound tones that every phone has and the environment that they are in.
- **Delivering the Banking Protocol** – a ground-breaking rapid response scheme through which branch staff can alert police and Trading Standards to suspected frauds taking place. The system is operational in every police force area and prevented £38 million in fraud and enabled 231 arrests in 2018.
- **Sponsoring a specialist police unit**, the Dedicated Card and Payment Crime Unit (DCPCU), which tackles the organised criminal groups responsible for financial fraud and scams. In 2018, the Unit prevented an estimated £94.5 million of fraud, secured 48 convictions and disrupted 11 organised crime groups.
- **Working with consumer groups** to develop a voluntary code to better protect customers and reduce the occurrence of [Authorised Push Payment] APP fraud. The code was published in February and will become effective for signatory firms on 28 May 2019.
- **Working with Pay.UK to implement Mule Insights Tactical Solution** (MITS), a new technology that will help track suspicious payments and identify money mule accounts, and Confirmation of Payee, an account name checking service for when a payment is made, that will help to prevent authorised push payment scams.
- **Hosting and part-funding the government-led programme to reform the system of economic crime information sharing**, known in the industry as Suspicious Activity Reports (SARs), so that it meets the needs of crime agencies, regulators, consumers and businesses.
- **Working closely with mobile network operators and the messaging industry to trial a new anti-spoofing system** to help root out scam text messages.
- **Helping customers stay safe from fraud and spot the signs of a scam** through the Take Five to Stop Fraud campaign, in collaboration with the Home Office.
- **Joining with government and law enforcement** to deter and disrupt the criminals responsible and better trace, freeze and return stolen funds.

- **Implementing new standards** to ensure those who have fallen victim to fraud or scams get the help they need.[52]

John Glen MP, Economic Secretary to the Treasury and City Minister, set out what the Government was doing to address banking fraud in response to a Parliamentary Question from Jim Cunningham MP in October 2018. He referred to action to address APP fraud, investment in Action Fraud and the Banking Protocol:

> The Government takes fraud very seriously and is determined to make it more difficult for fraudsters to operate.
>
> The independent financial services regulator – the Financial Conduct Authority (FCA) – requires banks to maintain effective systems and controls to prevent the risk that they might be used to further financial crime. This includes controls to prevent fraud. Under the Money Laundering Regulations firms must carry out customer due diligence measures to identify customers and check that they are who they say they are. If the FCA found evidence that a regulated firm did not undertake appropriate due diligence checks, that firm would be in breach of the Money Laundering Regulations and the FCA could consider what regulatory tools might be appropriate under such circumstances.
>
> The Government also supports the work that the Payment Systems Regulator (PSR) is driving forward, in conjunction with industry, consumer groups and other regulatory and Government bodies, to tackle Authorised Push Payment scams, in which individuals are tricked into sending money online. In April this year, the PSR established a Steering Group of financial institutions and consumer representatives to develop an industry code to help prevent these kinds of scams. In September, the Steering Group published the draft code for consultation and intends to finalise the code in early 2019.
>
> It is also important that victims of fraud are provided with adequate support, and that the public is equipped with the information they need to spot a scam and stand up to fraudsters. That's why the Government has invested in a new IT system for Action Fraud, which is the UK's national reporting point for fraud and cybercrime. This new system will deliver significant improvements, both for victims reporting fraud and cybercrimes, and for law enforcement in investigating these crimes.
>
> The banking industry has also taken important steps to prevent fraud, including through the Banking Protocol - a rapid response scheme through which branch staff can alert police and Trading Standards to suspected frauds taking place. 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 and led to 100 arrests.[53]

[52] "FRAUD THE FACTS 2019: The definitive overview of payment industry fraud", *UK Finance* [online], 21 March 2019 [accessed 8 April 2019]

[53] PQ182091 [on Banks: Fraud], 22 October 2019

4. Frequently asked questions

4.1 General

How do I reduce my chances of becoming a victim?

The Action Fraud website lists of different types of fraud. Under many of these it describes the actions that can be taken to reduce the risk from each type of fraud.

The website also sets out general advice for individuals and business.

The 'Take Five' website, which is a national awareness campaign led by industry and Government also offers advice to victimshttps://takefive-stopfraud.org.uk/advice/.

What should I do if I become a victim?

Action Fraud, which is the UK's national reporting centre for fraud and cybercrime, set out the actions that should be taken by victims of fraud. In short these involve reporting the crime to the police and notifying your bank:

> **First steps**
>
> The first thing you should do if you've been a victim of fraud is to contact Action Fraud. You can report a fraud via our online fraud reporting tool, or by calling Action Fraud on 0300 123 2040.
>
> If there is a crime being committed right now or if you are in danger you should call the police on 999.
>
> If debit or credit cards, online banking or cheques are involved, your first step should be to contact your bank or credit card company.
>
> **Ongoing support**
>
> When you report a fraud to Action Fraud, you are given the option for your contact details to be passed on to Victim Support, a national charity that helps those affected by crime. If you take up this option, you will then be contacted by someone from the charity and offered free and confidential emotional support and practical help.

4.2 Recovering losses

Can I recover lost money from my bank?

Only in certain circumstances can victims can recover their money from the card provider or bank.

For example, if someone used a credit card to pay for goods that never arrived, the card provider in most cases will provide a refund under the *Consumer Credit Act 1974*.

Which?, the consumer rights organisation, set out what victims can do to recover their money in different circumstances.

When can banks refuse to reimburse money?

Victims might not get their money back if the bank has reasonable grounds to think the victim was negligent with the security of their

account, or that they authorised the payment. For example, if the victim deliberately gave their password or PIN number to someone.

Banks might also refuse to refund losses if they happened 13 months or more before they were reported.[54]

The rules covering this issue are set out by the Financial Conduct Authority, which regulates financial providers.

Can a bank refuse to reimburse money if I was tricked into making the payment?

Possibly. In some banking scams victims are tricked into making payments to fraudsters (Authorised Push Payment – or APP). Reimbursement for these cases will be available provided the victim took appropriate care (such as taking heed of fraud warnings).

A new code for determining whether to reimburse victims was developed in 2018 and 2019 by industry and consumer groups.

Reimbursement will be contingent on whether banks and other payment service providers (PSPs) had met required standards (such as use of technology, rules and procedures) and whether the victim had taken a requisite level of care.

The aim of this approach is to:

> …establish better incentives for PSPs to take action to prevent and respond to APP scams, and for consumers to remain vigilant. This should help minimise the number of APP scams happening in the first place, but also reduce the impact on consumers when these scams do occur.[55]

The code came into force on 28 May 2019, although prior to then a draft code published in 2018 could already be taken into account by the Financial Ombudsman Service when determining complaints related to APP scams.[56] As of 22 May 2019, eight banks had signed the code.[57]

In cases where both the PSPs and customer involved did everything that was expected of them to prevent fraud (a 'no-blame' scenario), the customer will be reimbursed.

A long-term funding mechanism for delivering reimbursement to victims is in the process of being agreed by PSPs, with the intention for it to be fully in place by January 2020.[58]

---

[54] "Unauthorised payments from your account", *Financial Conduct Authority*, 13 January 2018 [accessed 8 April 2019]
[55] "What is the contingent reimbursement model?", *APP SCAMS STEERING GROUP*, accessed 8 April 2019
[56] "Authorised push payment scams: Outcome of consultation on the development of a contingent reimbursement model", *Payment Systems Regulator*, February 2018 [accessed 8 April 2019]
[57] "Eight banks sign new industry scam code: The latest UK Finance data shows that £354m was lost in the last year to bank transfer fraud", Financial Reporter, 22nd May 2019
[58] Personal communication with UK Finance, 11 June 2019

Can I appeal my banks decision not to reimburse me?

Yes. If a bank refuses to reimburse a victim a complaint can be made to the Financial Ombudsman Service (FOS). The FOS can investigate whether the bank took the correct decision, and whether it did enough to prevent the fraud.

More information about this process, along with the complaint application form, can be found here.

4.3 Police response

How can I find what progress has been made with my case?

Victims who have reported their case to Action Fraud should be able to access their report and track its progress on the Action Fraud website. The Action Fraud FAQ webpage includes a question on "I would like an update on my report?" which says:

> We have recently made some changes to our website. If you have made a report before the **6th October 2018** please get in contact with us to request an update.
>
> If you have recently registered on our new website, you can track the progress of your report by logging into your account. After logging in, to check your reports status click on "My account" in the top right-hand side of the website and then click "My reports".
>
> If you have any more queries, speak to us on web chat 24 hours a day.[59]

What communications should victims receive?

Action Fraud should send an automatically generated acknowledgement letter to each victim that reports a fraud case to them. This letter should include the victims 'crime reference number' and information about how their case will be handled through the NFIB.[60]

Victims who have reported their case directly to the police may also receive a letter from Action Fraud if their force has passed the case to them. Individual forces have responsibility for assigning a crime reference number and informing the victim of that number when they record a fraud case locally.

In theory, victims should receive their next communication from Action Fraud within 28 days.[61] This letter will explain whether the NFIB have allocated their case to a police force for investigation or not. In April 2019 the inspectorate of police forces stated that there was a three-month delay in NFIB staff analysing fraud reports.[62] Victims may not

---

59 Action Fraud, Frequently asked questions [last accessed 22 July 2019 11/07/19]
60 HMICFRS, Real lives, real crime: A study of digital crime and policing, December 2015, paragraph 9.12
61 Ibid, paragraph 9.13
62 HMCFRS, Fraud: Time to Choose: An inspection of the police response to fraud, April 2019, p15

receive an update from Action Fraud until the NFIB has analysed their case.

If a case is assigned to a police force for investigation that force should inform the victim if they are launching an investigation or not. The Code of Practice for Victims of Crime requires police forces to communicate with victims when they have arrested or charged a suspect in connection with their case.[63] Investigators may choose to share more information with victims, but police officers often keep the details of their investigations secret for operational purposes.

Why is my local force not investigating my case?

When the NFIB think there is appropriate evidence to launch an investigation into a fraud case they allocate it to the force where there are lines of enquiry. For example, the police force area where an identified suspect lives. Sometimes the force allocated a case will be different to the victim's local force.

The police have decided not to investigate my fraud case. Is there anything I can do?

Individual police forces may decide that there is not enough evidence to launch an investigation into a fraud report. Action Fraud and the National Fraud Intelligence Bureau (NFIB) may also decide that there is not enough evidence to pass a fraud report to a police force for investigation.

It is extremely difficult to challenge operational decisions taken by the police – including decisions on whether to allocate resources to investigate a particular reported crime. Such decisions are taken by the police (exercising operational independence) on a case by case basis. The police will consider the available resources and evidence and lines of enquiry. There is not much that can be done to force the police to investigate a particular case.

There is no specific process for challenging either a decision by a force not to investigate a fraud report or a decision by the NFIB not to pass a report to a local force. However, there are systems for members of the public to complain if they think the police have mishandled their case.

The FAQs section of Action Fraud's website includes details of how to complain about an Action Fraud Adviser and how to complain about a member of the NFIB. Action Fraud has also published Making a complaint to Action Fraud, which sets out some further details. The Library paper Police complaints systems in the UK describes the process of complaining about a local police force.

63 Ministry of Justice, Code of Practice for Victims of Crime, October 2015, pi

BRIEFING PAPER
Number 8545
22 July 2019

About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publicly available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email hcenquiries@parliament.uk.

Disclaimer