HOUSE OF COMMONS LIBRARY

BRIEFING PAPER

Number 8545, 23 February 2021

Banking fraud

By Jennifer Brown and Ali Shalchi

Contents:

Contents

Summary

Criminals successfully stole over £1.2 billion from individuals through banking fraud and scams in 2019.[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 2019 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 2019, only 25.4% of losses from authorised payments (£116m) 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 voluntary code of practice introduced in May 2019 gave a commitment, from all firms signed 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] There are calls for this code to be made mandatory.

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;

---

[1] "FRAUD THE FACTS 2020: The definitive overview of payment industry fraud", *UK Finance* [online], 18 March 2020 [accessed 16 February 2021]

[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]

- describes the different types of fraud;
- 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 victims.

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 there has been a "huge growth in fraud being driven by online adverts and social media content."[5]

It has been reported that criminals are increasingly using 'social engineering' techniques to bypass bank security measures. 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.[6]

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 over £1.2 billion through banking fraud and scams in 2019.[7]

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

- losses totalled £824.8 million, an decrease of 2 per cent compared to 2018.
- Banks and card companies detected and prevented £1.8 billion of unauthorised fraud losses. That equated to around £6.88 in every £10 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:

---

[4] "APP Scams Steering Group Agrees Voluntary Code", *APP SCAMS STEERING GROUP,* 28 February 2019 [accessed 8 April 2019]
[5] "FRAUD THE FACTS 2020: The definitive overview of payment industry fraud", *UK Finance* [online], 18 March 2020 [accessed 17 February 2021]
[6] "FRAUD THE FACTS 2020: The definitive overview of payment industry fraud", *UK Finance* [online], 18 March 2020 [accessed 17 February 2021]
[7] "FRAUD THE FACTS 2020: The definitive overview of payment industry fraud", *UK Finance* [online], 18 March 2020 [accessed 17 February 2021]

- Overall losses were £455.8 million (significantly up from £354.3 million the previous year). This was split between personal (£317.1 million) and nonpersonal or business (£138.7 million).
- 25.4% of losses (£116 million) 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 122,437 cases relating to a total of 121,658 victims. Of this total, 114,731 cases were on personal accounts and 7,706 cases were on non-personal accounts.

More information about the scale of different types of scam can be found in Fraud the Facts 2020, by UK Finance.

2. How do the police respond to fraud?

2.1 National coordination on fraud

Police coordination

Most fraud cases are investigated by local police forces. However, there are three policing bodies with national functions connected to fraud.

The City of London Police is the "national policing lead for fraud". It has set a national fraud policing strategy in collaboration with the National Police Chiefs Council (the coordinating body for UK police forces). It also runs a nationwide system for reporting and recording fraud.[8] It receives two annual grants from the Home Office to carry out these duties. In 2020/21 the CoLP received £2.5 million from the Home Office to carry out its duties as the "national policing lead for fraud" and £10.5 million to run the nationwide system for reporting fraud.[9]

The National Economic Crime Centre (NECC) is a unit within the National Crime Agency. It coordinates the UK's response to economic crime. The NECC is involved in both criminal and civil enforcement. They work with HMRC, the Financial Conduct Authority, the Serious Fraud Office and others to prioritise and task criminal and civil economic crime investigations. They also disseminate intelligence on and best practice for investigating economic crime to enforcement agencies.[10]

The Serious Fraud Office (SFO) investigates a small number of large complex economic crime cases in England, Wales and Northern Ireland.[11]

Government coordination

The Home Office has established a **Joint Fraud Taskforce** and an **Economic Crime Strategic Board** to coordinate action against fraud.

The Joint Fraud Taskforce (JFT) was established in February 2016.[12] The JFT works with law enforcement and the finance industry to tackle and prevent fraud.[13] There have been longstanding concerns that the JFT is ineffective. These concerns are discussed in greater detail in section 3.1 of this paper.

The Economic Crime Strategic Board was established in January 2019. 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 Government's Serious and Organised Crime Strategy (published in

8 NPCC, National fraud policing strategy 2019-2022, p8
9 City of London Police, Funding, [last accessed 17 February 2021]
10 NCA, National Economic Crime Centre, [last accessed 5 February 2020]
11 Serious Fraud Office, About us [last accessed 5 February 2020]
12 Joint Fraud Taskforce, The Joint Fraud Taskforce newsletter: Edition 1, January 2017
13 Ibid

November 2018). It will also scrutinise how well industry and law enforcement tackle economic crime.

In July 2019 the Board published an Economic Crime Plan 2019-22. Actions 26 to 29 of the plan's 52 actions are about 'enhancing the response to fraud'. These actions commit[14]:

- The Home Office, the CoLP and the NEEC to address the current deficiencies in the law enforcements response to fraud. The CoLP's national fraud policing strategy 2019-2022 addresses most of these concerns.
- The Home Office through the JFT to consider an "updated model for support for victims of fraud" by August 2020.
- The JFT to address "vulnerabilities that criminals exploit to conduct fraud" by December 2020.
- The Cabinet Office to build a "counter fraud profession" by April 2021.

More information about the Economic Crime Plan can be found in our briefing Economic crime in the UK: a multi-billion pound problem.

2.2 Reporting fraud

All cases of fraud should be reported to the City of London Police (CoLP). The CoLP is home to two national units, Action Fraud and the National Fraud Intelligence Bureau (NFIB), where fraud cases from across England and Wales are recorded and analysed. These units assign fraud cases to individual police forces for investigation.

There are limited circumstances in which a police force can record a fraud case locally and launch an investigation without analysis from CoLP. Normally, for a force to do so, the case should be "local" and officers should be able to easily identify suspects.[15] Police forces should still inform CoLP of cases they have recorded locally.[16]

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.[17]

Action Fraud's "contact centre" is managed, under contract, by a private company called Concentrix. The contract was previously held by

14 HM Govt & UK Finance, Economic Crime Plan 2019-22, July 2019, p43-44
15 Home Office, Counting Rules for Recorded Crime: Fraud, April 2019
16 Ibid
17 Action Fraud, What is Action Fraud? [last accessed 22 July 2019]

the not-for-profit organisation *Broadcasting Support Services,* but this organisation went into administration in 2015.[18]

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.[19] If not, they will log the case on NFIB systems and inform the victim (through Action Fraud) that no further action will be taken.[20] Frequently asked questions about this system can be found in section four of this briefing paper.

When the NFIB does allocate a case for police investigation it provides an "intelligence package" to the local police force assigned the case. These packages are designed to support local forces investigate the case. 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.[21] 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".[22] This system prioritises which cases will be reviewed by NFIB staff.[23]

2.3 Investigating fraud

Most fraud investigations are conducted by local police forces. Local police forces have operational independence. They can choose whether or not to launch and continue an investigation into a fraud case based on the available evidence and their resources.

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 it publicly available.[24]

Individual police forces handle fraud cases differently. Some have dedicated teams which investigate fraud, others allocate fraud cases to

18 House of Commons Home Affairs Committee, Policing for the future: Tenth Report of Session 2017–19, October 2018, paragraph 47
19 Ibid, paragraph 9.10
20 HMICFRS, Real lives, real crime: A study of digital crime and policing, December 2015, paragraph 9.13
21 Ibid, paragraph 9.7
22 Ibid, paragraph 9.9
23 Home Office, The scale and drivers of attrition in reported fraud and cyber-crime: Research Report 97, June 2018, p11
24 College of Policing, Investigation: Investigating fraud, January 2019 [last accessed 22 July 2019]

teams that specialise more widely in economic crime. Some forces have no specialist resource for investigating fraud at all.[25]

Regional Economic Crime Teams (teams based in Regional Organised Crime Units[26]) can assist local forces investigating complex fraud cases. However, their capacity is "extremely limited". The teams were set up to investigate fraud elements of other serious and organised crime investigations rather than to investigate standalone fraud cases.[27]

[25] HMCFRS, Fraud: Time to Choose: An inspection of the police response to fraud, April 2019, p11-12

[26] There are nine Regional Organised Crime Units (ROCUs) in the England & Wales. Neighbouring forces pool their resources to fund and administer ROCUs. ROCUs investigate organised crime across the police force areas they serve.

[27] NPCC, National fraud policing strategy 2019-2022, p7

3. Concerns about the 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.[28] When cases do reach the threshold for investigation police forces have often struggle to bring offenders to justice. Estimates suggest that as little as 3% of cases reported to Action Fraud result in charges or summons being brought against an offender.[29]

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".[30]

Her Majesty's Inspectorate of Constabulary, Fire and Rescue Services (HMICFRS) published an inspection of the police response to fraud in April 2019. The Inspectorate described some police practices investigating fraud as "intolerable".[31] They concluded that leaders in government and police forces now need to choose between the status quo where victims are "confused and disillusioned" or acting to ensure there is "a clearer strategy, less variation in service between forces and better communication with the public" on fraud.[32]

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 has meant that forces have failed to develop the specialist skills needed to investigate it. This has resulted in a large number of poor-quality fraud investigations.

3.1 Co-ordinating the police response to fraud

National fraud policing strategy

HMICFRS have been critical of government and the policing community for failing to develop a national strategy for fraud. In their 2019 inspection of the police response to fraud they recommended that the

28 Home Office, The scale and drivers of attrition in reported fraud and cyber-crime: Research Report 97, June 2018
29 House of Commons Home Affairs Committee, Policing for the future: Tenth Report of Session 2017–19, October 2018, paragraph 57
30 House of Commons Home Affairs Committee, Policing for the future: Tenth Report of Session 2017–19, October 2018, paragraph 66
31 HMCFRS, Fraud: Time to Choose: An inspection of the police response to fraud, April 2019, p5
32 Ibid

NPCC develop a national policing strategy for fraud and ensure it is adopted by all police forces by March 2020.[33]

Following this recommendation, the City of London Police (CoLP), through the National Police Chiefs Council's 'economic crime' portfolio, published the National Fraud Policing Strategy 2019-2022. The CoLP coordinated with the Home Office and the National Economic Crime Centre on the strategy. It was adopted by the NPCC, and therefore all 43 territorial police forces in England & Wales, in October 2019.

Should fraud be investigated by local police forces?

Some policing stakeholders have argued that local forces should not be responsible for investigating fraud. These stakeholders argue that regional or national investigative teams would be better suited to investigate fraud because fraud offending often crosses police force boundaries. They also argue that local police forces lack the capacity and capability to effectively investigate fraud.

The Home Affairs Select Committee rhave 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.[34]

The Police Foundation (a policing policy thinktank) agree with the Home Affairs Select Committee. 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.[35]

In contrast HMICFRS have concluded that the "current model of local investigations supported by national functions is the right one".[36]

The National Fraud Policing Strategy 2019-2022 sets out how the current system for investigating fraud will be improved so that local and national actors can work together more effectively. In the strategy the CoLP commits to creating "new coordination structures" including a National Strategic Coordination Group to bring together regional leaders and an Economic Crime Threat Group in each region to sit underneath it. Local police forces will be represented at these regional Economic Crime Threat Groups.[37]

The strategy also sets out a long-term ambition to bring together fraud, cyber and financial investigation capabilities to create "digital economic crime hubs".[38]

What's happening with the Joint Fraud Taskforce?

---

33 HMICFRS, Fraud: Time to Choose: An inspection of the police response to fraud, April 2019, recommendation 5, p44
34 House of Commons Home Affairs Committee, Policing for the future: Tenth Report of Session 2017–19, October 2018, paragraph 66
35 The Police Foundation, More than just a number: Improving the police response to victims of fraud, December 2018, p81
36 Ibid, p4
37 NPCC, National Fraud Policing Strategy 2019-2022, October 2019, p10
38 Ibid, p13

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".[39] 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.[40]

The last published meeting minutes for JFT's management board are from June 2018.[41] 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 assessment of fraud would be undertaken and that a new programme plan for JFT would be developed based on it.[42]

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.[43]

The JFT has yet to publish anything in relation to the threat assessment committed to in June 2018.

The JFT was given two specific 'actions' in the National Economic Crime Plan 2019-22.[44] They were tasked to:

- consider an "updated model for support for victims of fraud" by August 2020; and,
- address "vulnerabilities that criminals exploit to conduct fraud" by December 2020.

The NPCC's National fraud policing strategy 2019-2022 says that the City of London Police, the National Economic Crime Centre and the JFT will "work in partnership… to create detailed plans to tackle enablers of high harm fraud threats by March 2020".[45]

3.2 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".[46]

---

39 House of Commons Home Affairs Committee, Policing for the future: Tenth Report of Session 2017–19, October 2018, paragraph 71
40 NAO, Online fraud, June 2017, paragraph 2.14
41 Joint Fraud Taskforce, Management board minutes of meeting held 20 June 2018, June 2018
42 Ibid
43 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
44 HM Govt & UK Finance, Economic Crime Plan 2019-22, July 2019, p44
45 NPCC, National Fraud Policing Strategy 2019-2022, October 2019, p11
46 House of Commons Home Affairs Committee, Policing for the future: Tenth Report of Session 2017–19, October 2018, paragraph 50

In its 2019 inspection of the police response to fraud HMCFRS 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. [47]
- Delays of up to three months in NFIB staff carrying out case reviews on crime reports passed to them by Action Fraud.[48]
- Instances where the NFIB took up to four weeks to review a force request for a case to be reallocated.[49]

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 were not regularly investigating it."[50] They also found that regular reports on the fraud threat level were not being consistently used by forces because police staff found them unhelpful.[51]

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.[52]

The Government has insisted that "victims are receiving a much-improved service" from Action Fraud thanks to a new online reporting service.[53] The Government invested £5.5million in a new online reporting system for Action Fraud that went live in 2018.[54]

The CoLP and NPCC have committed to developing a "consent based model" for tasking fraud investigations. The aim of this model is to improve the tasking of fraud investigations by the NFIB to local forces. It is hoped this model will ensure the right cases are prioritised and work is not duplicated across the system.[55]

3.3 Quality of investigations

The 2019 inspection of the police response to fraud found "significant problems with the way fraud is currently investigated, including numerous examples of inefficient and ineffective processes."[56] The

47 HMCFRS, Fraud: Time to Choose: An inspection of the police response to fraud, April 2019, p12
48 Ibid, p15
49 Ibid
50 Ibid, p16
51 Ibid, p9
52 Ibid, recommendation 4
53 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
54 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
55 NPCC, National fraud policing strategy 2019-2022, p13
56 HMCFRS, Fraud: Time to Choose: An inspection of the police response to fraud, April 2019, p65

inspectorate highlighted some specific problems with current police practice:

- 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.[57]

HMICFRS 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.[58]

[57] HMCFRS, Fraud: Time to Choose: An inspection of the police response to fraud, April 2019, pages 65-80
[58] Ibid, recommendation 6

4. Industry and Government action on banking fraud

Information about how bank fraud is being tackled in the context of wider economic crime can be found in our briefing Economic crime in the UK: a multi-billion pound problem. The information provided below refers to fraud-specific action only.

4.1 UK Finance report

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 £49.1 million in fraud and enabled 253 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 2019, the Unit prevented an estimated £31.2 million of fraud, secured 75 convictions and disrupted 23 organised crime groups.
- **The introduction in May 2019 of a voluntary code** to help protect customers against APP fraud and reduce the number of cases, as well as treat customers more consistently. A fund set up by the banks that are signatories to the code means customers who fall victim to APP fraud despite having taken precautions will be reimbursed. The fund is in place until the end of this year. However, customers may also be refunded in other ways including by banks that have not signed up to the code.
- **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
- **The implementation, with Pay.UK, of Confirmation of Payee** (CoP), 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.

- **Helping customers stay safe from fraud** and spot the signs of a scam through the Take Five and Don't Be Fooled campaigns.
- **Working collaboratively** with other sectors including the telecoms industry, to address vulnerabilities in the ecosystem.[59]

4.2 The Voluntary Code on APP fraud

In 2018 the Payment Systems Regulator (PSR), a subsidiary of the Financial Conduct Authority,[60] set up a steering group of industry and consumer representation, to develop a voluntary code to assist victim of APP fraud. On 28 May 2019 a new voluntary code, the 'Contingent Reimbursement Model Code' (the Code) was established.[61] Payment Service Providers (such as banks) who signed up to the Code agreed that anyone who falls victim to APP fraud in circumstances where it wasn't reasonable to expect them to have protected themselves should be given their money back.

It most obviously applies to people using their personal bank accounts to make payments in the UK, provided those accounts are not used for trade or business. It also applies to certain small businesses and charities. But it doesn't apply to payments made using cash, cheque, credit or debit cards.

A customer who finds themselves falling victim to an APP scam, and whose bank has signed up to the Code, should report it to their bank as soon as possible. They can expect to be asked questions about the scam and why they were fooled into making the payment. The bank will then consider whether the customer took the care that was expected of them (on a case-by-case basis), and make a decision (ordinarily within 15 business days) on whether to reimburse that customer. If a customer is unhappy with the decision of their bank, they can make a formal complaint to the bank; and if they are dissatisfied with the bank's response, they can ask the Financial Ombudsman to look into the complaint.[62]

When the Code first launched in May 2019 the following banks and building societies had signed up: NatWest, RBS, Lloyds Banking Group, Barclays, HSBC, Santander, Metro, Nationwide and Starling Bank.[63] Consumer group Which? reports that the following are now also signed-up: Bank of Scotland, Cahoot, Cater Allen Limited, the Co-op, First Direct, Halifax, Intelligent Finance, M&S Bank, and Ulster Bank.[64]

---

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

60 See the governance section of the Payment Systems Regulator's website

61 APP scams, Payment Systems Regulator, last updated 11 February 2011 [accessed 17 February 2021]

62 Authorised Push Payment Scam – Information for Customers on the Voluntary Code, Lending Standards Board [online], undated [accessed 17 February 2021]

63 According to NatWest bank – see What other banks are signing up to the Authorised Push Payment (APP) Scam Code?

64 What to do if you're the victim of a bank transfer (APP) scam, Which? [accessed on 17 February 2021]

Major institutions that have not signed up to the Code therefore include Clydesdale Bank, Monzo, Post Office Bank, Tesco Bank, and TSB. In TSB's case, this is likely because it has a separate Fraud Refund Guarantee in place which refunds customers who are innocent victims of fraud.[65] Others who may not have signed up to the Code may still seek to informally upholds its standards, and therefore affected customers may still be able to turn to their bank for help.[66]

Reaction to the Code

The Guardian reported on 7 February that only a quarter of claims made under the Code were fully refunded. It also said that funding to compensate blameless victims under the Code will end on 30 June 2021. Following this date it is expected that a more sustainable funding model will have been decided upon by regulators, but it's unclear what will happen. The Treasury said it is considering what steps to take, including legislative changes. Which? said that "The voluntary nature of the scams code has allowed banks signed up to it to interpret and implement it in a wide variety of ways, without proper regulatory oversight".[67]

On 20 May 2019, shortly before the Code took effect, Liberal Democrat peer Baroness Ludford, in an oral question in the House of Lords, asked the Government "what further action they propose to take, and for banks to take, to prevent fraud perpetrated on bank customers." Speaking for the Government, Lord Young said:

> The voluntary code that comes into effect next week will in fact extend to all banks the facility to which the noble Baroness just referred, which has been undertaken by the TSB. As from next week, as long as you have done everything that you should and it was not your fault, you will get your money back. Vulnerable victims will get their money back even if they have not exercised due care. I welcome this not just because it gives added protection to customers, but because it means that the banks will have to pick up the bill, which will add to their incentive to reduce, so far as possible, incidents of fraud.

Lord Young added:

> Three initiatives are being taken by banks: confirmation of payee; the interception or interrogation of large sums; and the voluntary code. I will reflect on what the noble Baroness said and see whether there is a case for legislation, but we are making good progress with the steps I announced.[68]

On 11 February 2021 the Payment Systems Regulator announced that it was considering three proposals to help ensure that "people don't become victims [of APP scams] in the first place and, where someone does, that stronger protections are in place to help them". These proposals are:

---

65 See TSB's website for information on its Fraud Refund Guarantee

66 Monzo bank, for example, said in a tweet in May 2019 that it intended to sign up to the Code and until then would follow the "spirit" of the Code

67 Banks accused of letting down online fraud victims, *The Guardian*, 7 February 2021 [accessed 17 February 2021]

68 HL Deb 20 May 2019, vol 797, col 1770

> Making sure everyone can see how banks and building societies handle APP scams, by requiring them to publish their APP scam data, including reimbursement and repatriation (3) levels.
>
> Making it harder for fraudsters, by requiring banks and building societies to adopt a standardised approach to sharing data which will help identify these scams to stop them from happening in the first place.
>
> Extending customer protection across all banks and building societies at a minimum standard by changing payment system rules.

As part of these proposals, the PSR is considering extending the protections of the Code to make its terms mandatory for banks.[69] In November 2019 a Treasury Select Committee report recommended that the Code be made compulsory through legislation.[70]

4.3 Confirmation of Payee

Confirmation of Payee (CoP) is a name-checking service that warns customers when a payee's name doesn't match the account number they have provided.

Although banks typically used to ask for the name of the account holder to whom a payment is being sent, in reality it was only the account number and sort code that was used to direct the payment to the right recipient. This meant that someone entering the wrong account details could accidentally send money to the wrong person, or that fraudsters could use the name of a trusted organisation but ask you to make a payment to their account number and sort code. Which? estimated that CoP checks could have prevented £320 million of bank transfer fraud since 2017.[71]

In August 2019 the PSR issued a direction to the UK's six largest banking groups – Bank of Scotland and Lloyds, Barclays, HSBC, NatWest and RBS and Ulster Bank, Nationwide and Santander to implement CoP by 31 March 2020.

In November 2019 a Treasury Select Committee report looking into CoP concluded:

> Confirmation of payee will not solve economic crime alone, and as such the onus will always be on financial firms to develop further methods and technologies to keep up with fraudsters.
>
> The fact that banks were not previously confirming payees is a serious failure to protect customers from harm. Asking for such information but not using it would have created a false sense of security among some customers when sending payments. It might have been better for banks to not ask for this information at all if they were not going to use it for fraud prevention.

---

69 The PSR plans to bolster protections in payments, Payment Systems Regulator, 11 February 2021 [accessed 17 February 2021]

70 Economic Crime: Consumer View, Treasury Select Committee report, 1 November 2019, para 28

71 Confirmation of Payee: which banks are ready to offer vital name-checking service?, Which? [online], last updated 11 February 2021 [accessed on 18 February 2021]

> We therefore recommend that Confirmation of Payee should be introduced as a matter of urgency. Every delay leaves more people vulnerable to falling victim to economic crime. If the implementation date of March 2020 begins to look in doubt, regulators should consider introducing sanctions, such as fines, to firms who have not met the deadline.
>
> The arguments put forward that Confirmation of Payee implementation could be harmful for competition if large firms implemented before small ones, is without merit. Competition in the banking sector exists for the benefit of customers, not for the benefit of firms. Customers should not be put at risk of becoming victims of fraud, in order to protect slow adopting firms from implementing protections for their customers. The Payment Systems Regulator should therefore ensure that all relevant firms can implement Confirmation of Payee by the end of 2020.
>
> Subtle differences which might not be immediately obvious to many people, such as using 'soliciters' rather than 'solicitors', could represent a fruitful way for fraudsters to disguise fraudulent accounts as legitimate accounts, and therefore small inaccuracies should be flagged for consumers' own protection. We recommend that spelling mistakes are flagged within the new Confirmation of Payee System.[72]

In March 2020 the PSR announced that it would not take action against banks that failed to meet the March 2020 deadline for implementation until 30 July 2020, due to the coronavirus pandemic. In July 2020, the PSR confirmed that the six bank groups had "achieved widespread implementation" of CoP. The PSR now says it is encouraging banks and providers of all sizes to implement CoP.[73] Which? however has reported that some banks, including Metro Bank, have no plans to implement to CoP.[74]

Another key recommendation made by the November 2019 Treasury Select Committee report is:

> a mandatory 24-hour delay on all initial or first-time payments, during which time a consumer about to be defrauded could remove themselves from the high-pressure environment in which they are being manipulated. All future payments to that same account could flow at normal speed to minimise inconvenience to customers. If a situation arose whereby an initial payment was needed instantly, a customer could ring their bank and additional checks could be carried out for the funds to be released.[75]

---

72 Economic Crime: Consumer View, Treasury Select Committee report, 1 November 2019, paras 39 to 43

73 APP scams, Payment Systems Regulator [online], [accessed 18 February 2021]

74 Confirmation of Payee: which banks are ready to offer vital name-checking service?, Which? [online], last updated 11 February 2021 [accessed on 18 February 2021]

75 Economic Crime: Consumer View, Treasury Select Committee report, 1 November 2019, para 10

5. Frequently asked questions

These FAQs aim to support the work of MPs. You should not rely upon this information as legal or professional advice, or as a substitute for it. We do not accept any liability whatsoever for any errors, omissions or misstatements contained herein. You should consult a suitably qualified professional if you require specific advice or information. Read our briefing for information about sources of legal advice and help.

5.1 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 victims.

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.

5.2 Recovering losses

Can I recover lost money from my bank?

Only in certain circumstances can victims 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.[76]

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).

An industry-led voluntary code for determining whether to reimburse victims was established in May 2019 and there are calls to make it mandatory for all banks. For more information on how the code works see section 4.2 above.

Can I appeal my bank's 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.

5.3 Police response

There are four stages to the police response to a fraud report:

1 **Reporting**: A victim reports an incident of fraud. Victims should report fraud directly to Action Fraud (the national reporting centre for fraud). Fraud reported to local forces is likely to be passed to Action Fraud.

2 **Recording**: Action Fraud records fraud reports using Home Office counting rules. They pass *recorded* cases to the National Fraud Intelligence Bureau (NFIB). Reports that can't be recorded will progress no further.

[76] "Unauthorised payments from your account", *Financial Conduct Authority*, 13 January 2018 [accessed 8 April 2019]

3 **Allocating**: The NFIB analyse recorded fraud cases and allocate them to the most appropriate police force when there's appropriate evidence to warrant an investigation. Recorded cases that don't qualify for allocation will progress no further.

4 **Investigating**: Police forces assess the cases they're allocated and decide how to progress them. They may launch an investigation, decide not to launch an investigation or ask NFIB to reallocate the case to another force. Fraud cases will progress no further when the police decide not to launch an investigation.

Reporting and recording fraud

Action Fraud should send an automatically generated acknowledgement to each victim that reports a fraud case to them. Sometimes this acknowledgement will tell them their case hasn't been recorded. The police must follow Home Office counting rules to decide whether to record a fraud report. Some things people think of as fraud, such as phishing and identity theft, aren't fraud under the counting rules.

If a fraud report is recorded, the automatically generated acknowledgement will include the victim's crime reference number and information about how their case will be handled through the NFIB.

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.

Allocating recorded fraud cases to police forces

The NFIB will allocate recorded fraud cases to the most appropriate police force when there's appropriate evidence to launch an investigation. **Sometimes the force allocated a case will be different to the victim's local force.** This is because investigative lines of enquiry may be in another police force area.

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

Victims with recorded complaints should receive an allocation decision within 28 days. In April 2019 the inspectorate of police forces stated that there was a three-month delay in NFIB staff analysing fraud reports.[77] Victims may not receive an update from Action Fraud until the NFIB has analysed their case.

Investigating fraud

The police force assigned the case will decides how to progress the case. They can either launch an investigation, choose not to launch an investigation or (where appropriate) ask the NFIB to reassign the case.

Why would the police not investigate a fraud case?

There are many different reasons why fraud cases may not be investigated. For example, there may be a lack of available evidence or

the assigned force may decide that an investigation would not be a proportionate use of their resources.

Informing victims during an investigation

Investigators may choose to share more information with victims, but police officers often don't share information for operational purposes.

The police must tell the victim when they arrest or charge a suspect. The Library's casework page support for victims of crime explains more about how the police should treat victims.

Complaining

There is no specific process for challenging operational decisions regarding fraud. However, people can complain if they aren't happy with how the police handled their case.

Action Fraud have explained how people can complain about it on their website. It has also provided specific information about complaining about an Action Fraud Adviser and a member of the NFIB.

The Library's short guide to police complaints helps those supporting constituents who are dissatisfied with the police.

Further information

Action Fraud has provided information for the public about fraud on its website. This includes a series of Frequently Asked Questions and a guide to reporting fraud.

BRIEFING PAPER
Number 8545
23 February 2021

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