HOUSE OF COMMONS LIBRARY

BRIEFING PAPER

Number 8350, 26 June 2018

Action against bank account scams

By Timothy Edmonds

Contents:

Contents

Summary

Amidst all the advantages of electronic banking for customers, the undoubted 'fly in the ointment' is the prevalence of online fraud, especially authorised push payment (APP) scams.

The banking industry has a broad regulatory requirement to provide a safe banking environment and it is keen to help customers stop getting into trouble in the first place and do what it can to help if they have already fallen foul.

In terms of preventative measures, there is a widely advertised 'Take Five' campaign to encourage people to be sceptical about requests for them to send their bank details to unknown people or to change previously agreed payment details at the last minute.

In the process of being drawn up is a system of recompense for customers who have been subject to fraud. This will be available later in 2018.

With respect to more traditional frauds e.g. frauds on vulnerable people made by roofers or the like, the 'Banking Protocol' allows bank staff rapid access to police and other agencies if they believe that a person in their branch is withdrawing money that is the result of a fraud.

Customers are encouraged to contact Action Fraud and or the police if they think they have been defrauded. In limited circumstances victims might be able to go to the Financial Ombudsman if the bank has been negligent. The Financial Conduct Authority proposes to extend the remit of the Ombudsman to include such scams.

1. Introduction

Amidst all the advantages of electronic banking and the great ease with which customers can now make payments and transfer money to other accounts, the undoubted 'fly in the ointment' is the prevalence of online fraud and, especially, authorised push payment (APP) scams.

An APP scam is where the account holder themselves authorises the payment to be made to another account, believing it to be a genuine supplier or authority (e.g. HMRC). Once the fraud is discovered, the fraudster's account is empty and the fraudster gone.

Alternatively, fraudsters can intercept genuine accounts and receive payments direct that way. According to a Report by the Payment Systems Regulator (PSR) it was much more common for the victim to make a payment to a scammer direct, than the scams where the victim is duped into making a payment to the wrong account. The former appears to make up between 85% and 95% of total APP scams, although the average value of such scams tends to be smaller.[1] A Report by the Financial Conduct Authority (FCA) published in June 2018 gave two examples of APP fraud:

> **Example A:** B received 2 calls from someone pretending to be from his bank. They were asked whether they authorised 2 transactions in Manchester and London. B denied authorising these transactions and was told their account had been compromised. B was then told that, to protect their account, they needed to transfer money into a new account which turned out to be under the scammer's control. B ended up losing £18,700, which could not be recovered.
>
> **Example B:** S attempted to buy a motorhome online. S transferred £4,500 to the purported seller of the motorhome, who turned out to be a scammer. The motorhome was never provided. S told the police but the money could not be recovered.[2]

The sums lost through these scams is enormous.

1.1 Fraud data

Data on unauthorised payment frauds – a wider category than the main subject of this Paper – are collated by the banking industry and published by UK Finance. In 2017 it included, for the first time, data on 'push payment scams. It found:

- There were 43,875 reported cases of authorised push payment scams with a total value of £236.0 million. 88 per cent of this total were retail consumers, losing an average of £2,784, and the remainder were businesses who lost on average £24,355 per case.

---

1 Payment Systems Regulator: Which? authorised push payments super-complaint; December 2016

2 FCA; Authorised push payment fraud – extending the jurisdiction of the Financial Ombudsman Service; June 2018

- Financial providers were able to return £60.8 million (26%) of the authorised push payment scam losses in 2017.

Behind the overall figures lie numerous heart-breaking stories of vulnerable people losing their savings following a seemingly genuine telephone or internet request to take action to pay money to an alternative account for real services or to pay for non-existent bills..

2. Initiatives

The banking industry together with the enforcement authorities have established various procedures to limit the damage done by APP fraud. Some of this work – the preventative measures are embodied in agreed practices and inter agency contacts – normally summarised as being the Banking Protocol. Also, a model is being developed to provided compensation for customers where none exists presently.

2.1 Preventative measures

Take Five

The most public face of the preventative measures is the 'Take Five' Campaign described as being:

> Take Five is a national campaign that offers straight-forward and impartial advice to help everyone protect themselves from preventable financial fraud. This includes email deception and phone-based scams as well as online fraud – particularly where criminals impersonate trusted organisations. Led by Financial Fraud Action UK (part of UK Finance) and backed by Her Majesty's Government, it is being delivered with and through a range of partners in the UK payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector organisations.[3]

The 'five' is a call to take five minutes before responding to telephone calls, texts, emails or other communication where the main request appears to be for personal and banking information. For example, it suggests:

> • Banks or trusted organisations will never contact you asking for your PIN or full password, or to transfer money to a safe account.
>
> • Never give out your personal or financial details unless you are absolutely sure you know who you are dealing with.
>
> • Always question uninvited approaches asking for information – it could be a scam. Instead contact the company directly using a trusted email or phone number to check the request is genuine.
>
> • Don't be tricked into giving a fraudster access to your details. Never automatically click on a link in an unexpected email or text.

Although not strictly and directly connected with APP scams – although they can be linked - one should also note the impact of what is called the 'Banking Protocol'.

Banking Protocol

This has been piloted in 2016 and was rolled out nationally, beginning in May 2017. Its main focus is on intra branch activity, where individuals are withdrawing large sums to pay to fraudsters.

> The Banking Protocol enables bank branch staff to contact police if they suspect a customer is in the process of being scammed, with an immediate priority response to the branch. UK Finance has led the development and implementation of the scheme, which is a partnership between the finance industry and police

[3] Take Five Campaign website

> supported by National Trading Standards and the Joint Fraud Taskforce. Branch staff, call handlers, police and trading standards officers in each area have all been trained in the Banking Protocol and the steps that need to be taken when a customer is at risk.[4]

According to UK Finance:

> Since March 2018 it has been implemented by all 45 police forces across the country. In that time it has led to 197 arrests across the country, while 3,682 emergency calls have now been placed and responded to through the scheme, with the average prevention per call equating to £6,720. In May 2018, the Banking Protocol prevented over £3m in fraud – a monthly record – while 17 arrests were made.[5]

This initiative is aimed more at cases such as workmen demanding large cash sums for 'roof repairs'.

2.2 Compensatory measures

The Which? Super Complaint

The industry, in conjunction with consumer groups and the PSR, is currently working towards a more effective and consistent set of principles with respect to losses incurred due to APP scams when prevention has failed.

The work began with a 'Super Complaint' by Which? to the PSR and the Financial Conduct Authority (FCA) in September 2016.

The PSR's response to the complaint can be found here. It sets out the existing rights and responsibilities of banks described officially as payment service providers or PSPs in the text.

> While PSPs are not generally liable for APP scams, both sending and receiving PSPs are nonetheless under a range of obligations to prevent fraud. Existing legislation requires PSPs to 'know your customer', conduct due diligence, maintain appropriate records and to implement policies, procedures and training, with the aim of avoiding the facilitation of money laundering; requires PSPs to report financial crime in certain circumstances; and imposes a number of obligations on them concerning the safe use of so-called 'payment instruments' and payment instructions. The FCA's Handbook places additional obligations on certain PSPs, including banks, to have adequate policies and procedures to counter the risk that they might be used for financial crime, including fraud.
>
> Even if a PSP is not strictly liable under legislation, it may be required to compensate a customer for its losses by the Financial Ombudsman Service if the ombudsman service considers this to be fair and reasonable in the circumstances. The ombudsman service can hear any dispute arising out of the carrying on of a regulated activity. The ombudsman service has upheld complaints against both sending and receiving PSPs, though where an individual is not a customer of the PSP in question, the complaint must be sufficiently connected with the disputed payment.
>
> The available evidence suggests that current legal obligations and commercial incentives already mean that the sending bank's interests are broadly aligned with those of the consumer. While

4 UK Finance Press Release 22 June 2018
5 UK Finance Press Release 22 June 2018

> specific practices vary, in general sending PSPs appear to have developed reasonably extensive measures to help prevent their customers from falling victim to APP scams. We also observe that sending PSPs generally appear to make reasonable efforts to assist their customers in recovering funds they have transferred as a result of an APP scam. In some instances we observe sending PSPs voluntarily refunding victims for the funds lost as the result of a scam.[6]

The PSR noted that the interests of the banking industry were aligned with those of their customers, it was not a case that the banks simply wanted to ignore scams, but that there was uncertainty about how to proceed. The PSR recommended:

> We have sought to develop proposals that complement such work, making sure the issues we have identified are addressed. To that end, we have agreed with FFA UK a programme of work that the banking industry should lead on, that will assist in both understanding the scale of APP scams and in improving how PSPs work together in responding to them:
>
> - Industry, liaising with the Information Commissioner's Office as appropriate, to develop a common understanding of what information can be shared under the current law, and the key legal barriers to sharing further relevant information (for example, information that would help victims recover their money).
> - Industry to develop a common approach or best practice standards that sending and receiving PSPs should follow when responding to instances of reported APP scams. We would expect this to cover issues such as the availability of fraud specialists and processes for agreeing indemnity agreements between banks.
> - Industry to develop, collect and publish robust APP scam statistics, to address the lack of clear data on the scale and scope of the problem, and to enable monitoring of the issue over time.

In March 2017 the PSR published the terms of reference for its work with the industry. What has resulted is, published in February 2018, its Authorised push payment scams: Outcome of consultation on the development of a contingent reimbursement model. The Executive summary outlines work done and future progress:

> Taking account of responses, we consider that an industry code, developed collaboratively by industry and consumer group representatives, that sets out the CRM's rules is the most effective way to promote the interests of users of payment system services and reduce the consumer harm that APP scams can cause.
>
> […]
>
> We are bringing the right people together to establish a dedicated steering group to develop the code. The steering group will have an equal balance of representatives from key stakeholder groups, particularly consumer representatives and PSPs. We will drive the steering group forward and provide oversight and support, and other relevant regulatory and governmental bodies will also be

[6] Payment Services regulator: Which? authorised push payments super-complaint; December 2016

> involved as observers. The steering group will be responsible for reaching consensus between members on a set of key issues, and formalising the CRM into a set of rules that will form an industry code for reimbursement of APP scam victims.
>
> We have established a set of core principles for the code that we expect the steering group's proposals should be consistent with. These are principles that we consider underpin an effective CRM that should better protect consumers from harm. Amongst others, these include principles to provide the right incentives for those parties who can best reduce the occurrence of APP scams and respond to them, to deliver consistent outcomes for parties with the same circumstances, and to be based on measures that are likely to be effective at preventing and responding to APP scams.
>
> We have set out an ambitious timeline for the steering group. We want it to produce an interim code by September 2018 that the Financial Ombudsman Service can start taking into account as a relevant consideration when determining consumer complaints about APP scams. The steering group – following a final round of consultation – should have the final code in place in early 2019. This timeline recognises the need to address the significant harm being caused by APP scams as soon as possible, alongside the importance of developing an effective model that does not result in any foreseeable unintended consequences for users of push payments.[7]

The upshot of this work is two-fold.

Consultation on general directions for the implementation of Confirmation of Payee (COP)

[Note in banking terms payee is the person receiving funds] This is the outcome of the work by all sides of the industry to find a technical solution to push payment scams. In the accompanying press release the PSR say:

> The PSR has always been clear that more needs to be done to protect people from Authorised Push Payment (APP) scams and CoP is one important tool for preventing these scams. Together with the new, voluntary industry code, designed by the industry and consumer groups, CoP will see consumers better protected from APP scams and have a greater chance of being reimbursed if they do fall victim.
>
> CoP is the industry-agreed way of ensuring that names of recipients are checked before payments are sent. It will work by checking the account name and account details to make sure there is a match. Alerts will notify the payer whether there has been a match or not, meaning corrections can be made before the payment is made.
>
> We are considering regulatory intervention to ensure that PSPs implement CoP.

The full document can be seen here. In brief CoP:

---

7 PSR; Authorised push payment scams: Outcome of consultation on the development of a contingent reimbursement model; February 2018

> is a service which when introduced should reduce significantly the incidence of APP scams and accidentally misdirected payments.
>
> When people set up payments from their account, their PSP often asks them to give the recipient's name, sort code and account number. The customer may expect the PSP to check all three of these during the transaction. However, the name is not checked. Therefore, a payment will not be stopped or returned if the name of the payee does not match the name of the intended recipient.
>
> If payers were able to compare the name on the receiving account with their intended recipient, they would have a much better chance of avoiding scams or misdirected payments.
>
> CoP is the industry-agreed way of ensuring that names of recipients are checked before payments are sent, so the payer can be confident that the payee is who they expect it to be.[8]

Voluntary Industry Code

This was published in September 2018 and is still in draft form. The authors state:

> The draft voluntary code aims to make it harder for criminals to commit this type of fraud, sets out how consumers can be vigilant and take reasonable steps to protect themselves whilst giving them greater levels of protection and support from their banks. Importantly, the code proposes the principle that where a consumer has met their requisite level of care, they should be reimbursed. It has been developed and proposed with the principles of fairness, simplicity and transparency at its core.
>
> Under the draft code, each bank and other payment service providers (PSPs) would take measures to tackle APP scams, such as:
>
> **Detecting** APP scams through measures such as analytics and employee training
>
> **Preventing** APP scams from taking place by taking steps to provide customers with effective warnings that they are at risk
>
> **Responding** to APP scams, for instance by delaying a payment while an investigation is conducted and if necessary, carrying out timely reimbursement[9]

The consultation period is now over, so we wait to see what emerges.

The Financial Ombudsman

Although individuals can take cases involving scams to the Financial Ombudsman, the grounds for doing so are rather restricted. For example, it cannot currently consider complaints by payers made against the banks that have received funds transferred due to APP fraud.[10]

---

8 Op cit p4

9 The APP Scams Steering Group; **CONTINGENT REIMBURSEMENT MODEL**; press release September 2018

10 A selection of cases that it can look at can be found in this edition of Ombudsman's News, which is a thematic review of cases that it has dealt with.

In June 2018 the FCA published a Consultation Paper that would make APP scams referable to the Ombudsman in the normal way. The Paper - Authorised push payment fraud – extending the jurisdiction of the Financial Ombudsman Service had two proposals:

- applying our complaint handling rules to complaints brought by a payer in relation to the alleged failure of a receiving PSP in a payment transaction to prevent or respond to an alleged APP fraud, and bringing these complaints into the Financial Ombudsman Service
- bringing complaints about the failure of the receiving PSP to cooperate with the sending PSP in recovering a misdirected payment into the Financial Ombudsman Service's CJ and VJ

The FCA hopes that by making compensation more readily available that PSPs (banks) will be more vigilant in their monitoring of new customers, although it warns that this could have "the effect of making opening an account or requesting a push payment more complex". Many people already struggle to 'prove who they are' with banks, and more routine payments may generally become less simple to effect.

The Financial Ombudsman produces a regular round up of its cases thematically in its 'Ombudsman's News publication. In August 2018 the subject was phishing scams. In the introduction, the Chief Ombudsman wrote:

> Unlike most other complaints we see, complaints about fraud and scams involve – whether it's accepted or suspected – the actions of a criminal third party. So it's understandable that, in many cases, both the bank and their customer tell us in strong terms that they're not responsible for what's happened.
>
> This makes it harder for us to reach an answer both sides are happy with. But it doesn't mean usual standards don't apply. As our case studies illustrate, we'll expect to see clear evidence that banks have investigated thoroughly – and reflected hard on what more might have been done to protect their customers and their money.
>
> We also often hear from banks that their customers have acted with "gross negligence" – and this means they're not liable for the money their customer has lost. However, gross negligence is more than just being careless or negligent. And as our case studies show, the evolution of criminals' methods – in particular, their sophisticated use of technology and manipulative "social engineering" – means it's an increasingly difficult case to make.[11]

The publication includes a number of case studies which illustrate what the Ombudsman can and cannot do to provide compensation. An interesting take away from looking at these is that the more sophisticated is the scam the least likely it is that the Ombudsman will agree that the victim has been grossly negligent – the thing that banks have to prove or rely upon to avoid liability.

---

[11] Financial Ombudsman website August 2018

BRIEFING PAPER
Number 8350
22 June 2018

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