Authorised Push Payment Scam – Information for Customers on the Voluntary Code

This guide explains how the new Authorised Push Payment (APP) Scam Voluntary Code works.

If you are worried that you might have been a victim of a scam it is important to make contact with your bank, building society or other payment provider immediately, using the number on the back of your debit, credit or prepaid card or by visiting their website. The sooner you make contact the more chance you have of getting your money back so don't delay or try to check things out yourself.

If you have been a victim of a scam and don't have access to any money because it's all been taken, tell your bank as they may be able to help you. You can also contact the Citizens Advice consumer helpline: 03454 04 05 06 www.citizensadvice.org.uk/consumer/get-more-help/if-you-need-more-help-about-a-consumer-issue/

If you have been a victim of a scam and are finding it hard to recover from the experience, contact Victim Support on 08 08 16 89 111 or by visiting www.victimsupport.org.uk

What is the Authorised Push Payment (APP) Scam Voluntary Code?

From 28 May 2019 Payments Services Providers will be able to sign up to a new voluntary code, known as the 'Authorised Push Payment Scam Code'. The term *Payment Services Provider* includes banks, building societies, credit unions, and electronic money and payments institutions. We are using the term 'bank' throughout this guide for simplicity, but when we do, it also includes these other payment services providers, as they may be involved in transferring your money.

You can ask your bank if it is signed up. The new APP Code aims to provide greater protection to customers from authorised push payment scams by increasing customer awareness and education, doing more to prevent these scams and by committing to reimburse customers in certain circumstances. **The Code does not guarantee that all customers will get their money back, you still need to take care when making payments.**

What is an authorised push payment scam?

Authorised push payment scams (sometimes called APP scams) are where someone is tricked into transferring money to a fraudster via a bank transfer. A bank transfer is an

electronic payment made out of your account. You can make bank transfers via your bank online or by mobile banking, or within a branch or by telephone banking. The APP Code only applies where you have made the payment yourself, or given someone you trust your password or let them access your account for the specific purpose of making the payment.

This APP Code doesn't apply if someone takes money from your account without your permission. Also, it does not apply if you have given someone permission to make a payment on your behalf and they have taken *more* money out than you said they could. This is known as unauthorised fraud. The Code also doesn't apply to payments made using cash, cheque, credit, debit or prepaid card. You can find out more about your rights and unauthorised scams and credit/debit/prepaid card fraud from the Citizen's Advice Consumer Service: 03454 04 05 06 or www.citizensadvice.org.uk/consumer/get-more-help/if-you-need-more-help-about-a-consumer-issue/

There are many different kinds of APP scams, including:

- romance scams – fraudsters, typically using a fake profile, form a relationship in order to ask for money, or enough personal information to steal the victim's identity
- fraudsters who convince people to move money to a 'safe account' such as another bank account
- purchase scams – sending money to buy goods that don't exist
- invoice scams – where fraudsters send a false invoice, often pretending to be from a company that the victim is expecting a bill from

Does the Code protect me?

The Code applies to:

- Individuals' personal accounts providing they are not being used for trade or business
- Micro-enterprises: enterprises which employ fewer than 10 people and whose annual turnover and/or annual balance sheet total does not exceed 2 million euros
- Charities with an annual income of less than £1million
- Payments made within the UK, so it won't cover you if you send payments overseas

What will banks who sign up to the Code do?

Banks commit to take a number of steps aimed at protecting customers from APP scams, these include:

- Taking steps to educate their customers about APP scams
- Taking steps to identify higher risk payments and customers who have a higher risk of becoming a victim of APP scams
- Providing effective warnings to customers if the bank identifies an APP scam risk

- Taking extra steps to protect customers who might be vulnerable to APP scams
- Talking to customers about payments and even delaying or stopping payments where there are scam concerns
- Acting quickly when a scam is reported to it
- Taking steps to stop fraudsters opening bank accounts

Banks have also agreed to reimburse customers who have lost money to APP scams in some circumstances.

What do I have to do?

The decision about whether you get your money back should be made on the basis of your individual circumstances. So, **if at the time you made the payment, you really didn't believe it was a scam make sure you explain this to your bank.**

You do have a responsibility to take steps to protect yourself before you can expect to be reimbursed under the Code.

You will generally be expected to:

- Pay attention to warnings given to you by your bank. *Your bank might show you extra messages when you set up, change or make payments. It's very important that you pay attention to these and follow any instructions.*
- Have a reasonable basis for believing that:
    - The person you pay was the person you were expecting to pay
    - That the payment is for genuine goods or services
    - The person or business you are paying is legitimate

  Always think carefully before making a payment, especially if it's a lot of money for you. If you have any doubt about the payment or payment details, talk to someone you trust or call your bank using the number on the back of your card.
- Take care – if you've been extremely careless then you shouldn't expect to get your money back. *Many people lose confidence and think they should have spotted the scam after they found out they've fallen for a scam. Don't let this put you off asking your bank to look into your case, the test is about what you did and thought at the time of the payment, not afterwards.*

In some cases, it may not be reasonable to expect people to have protected themselves from a particular scam or to have taken the steps set out above. There are many different reasons why someone might not have been able to protect themselves. It might be that the scam was so convincing and sophisticated that even someone who was experienced in making payments couldn't protect themselves.

The Code says that if the combination of a person's individual circumstances and the scam itself mean that it wasn't reasonable to expect that person to have protected themselves

then they should always be given their money back. The Code refers to these people as 'vulnerable to APP scams'. There isn't a tick list to decide if someone is vulnerable, it will always be decided on a case by case basis.

Your bank will probably ask you questions about the scam and what you did and to explain why you believed what you did at the time. They might also ask you to provide any evidence that is available to support what you have told them, for example phone records or copies of emails. They should always ask these questions sensitively and you should let them know if you need more support or for the bank to communicate with you differently. Remember that there are organisations that can provide independent advice and support in relation to the scam and the impact it has had on you. A list of organisations and their contact details is included at the end of this guide.

Some of these questions might feel personal and be difficult to answer, however it is important to be as open and honest with your bank as you can. The bank is trying to understand what went on at the time of the scam and whether you were vulnerable to the scam and also to get details that can help them protect other customers. If you do not provide the information the banks need or are dishonest when responding to questions after you have reported a scam, then the bank may decide that it will not reimburse you.

In what circumstances will I get my money back?

The Code requires that banks reimburse customers if they were vulnerable according to a definition set out in the Code, even if banks have also done everything they should have under the Code.

Banks that have signed up to the Code commit to give you all the money you lose to an APP scam if you have done what was expected of you as detailed in the section above.

You will get some, but not all, of your money if the bank has failed to provide the protections set out in the Code and you have also not done what was expected of you.

If the Bank has met the Code requirements and you did not take the care that was expected of you then you should not expect to get any money back, although a bank might choose to make a goodwill payment.

What do I do if I've lost money to an APP Scam?

Tell your bank as soon as possible if you think you might have sent money to an APP scam. Your bank will try to trace your money so the sooner you let them know the more chance you have of getting it back.

If your bank is a member of the Code then you should ask your bank to investigate whether you are entitled to get your money back under the Code. The bank should normally let you know within 15 business days (or 35 days in extraordinary circumstances).

If your bank is not a member of the Code then you can still ask your bank to investigate.

If your bank has told you that you're not entitled to get any money back but you think you should be then you might want to find out more information from the contacts below.

If you are not happy with the decision of your bank you should make a formal complaint to your bank. If you are not satisfied with the outcome of the complaint or you have not had an answer within 8 weeks, then you should ask the Financial Ombudsman Service to look into your complaint. This is a free service. For further information visit www.financial-ombudsman.org.uk or call 0800 023 4567.

Where can I go to get more help understanding this Code?

If you've experienced an APP scam and want more information about your rights, or help making a complaint, you can contact:

Citizen's Advice Consumer Service: 03454 04 05 06 or www.citizensadvice.org.uk/consumer/get-more-help/if-you-need-more-help-about-a-consumer-issue/

Which?: www.which.co.uk/consumer-rights/advice/what-to-do-if-youre-the-victim-of-a-bank-transfer-app-scam

Money and Pensions Service: 0800 138 7777 or www.moneyadviceservice.org.uk/en

Age UK: 0800 678 1602 or www.ageuk.org.uk/