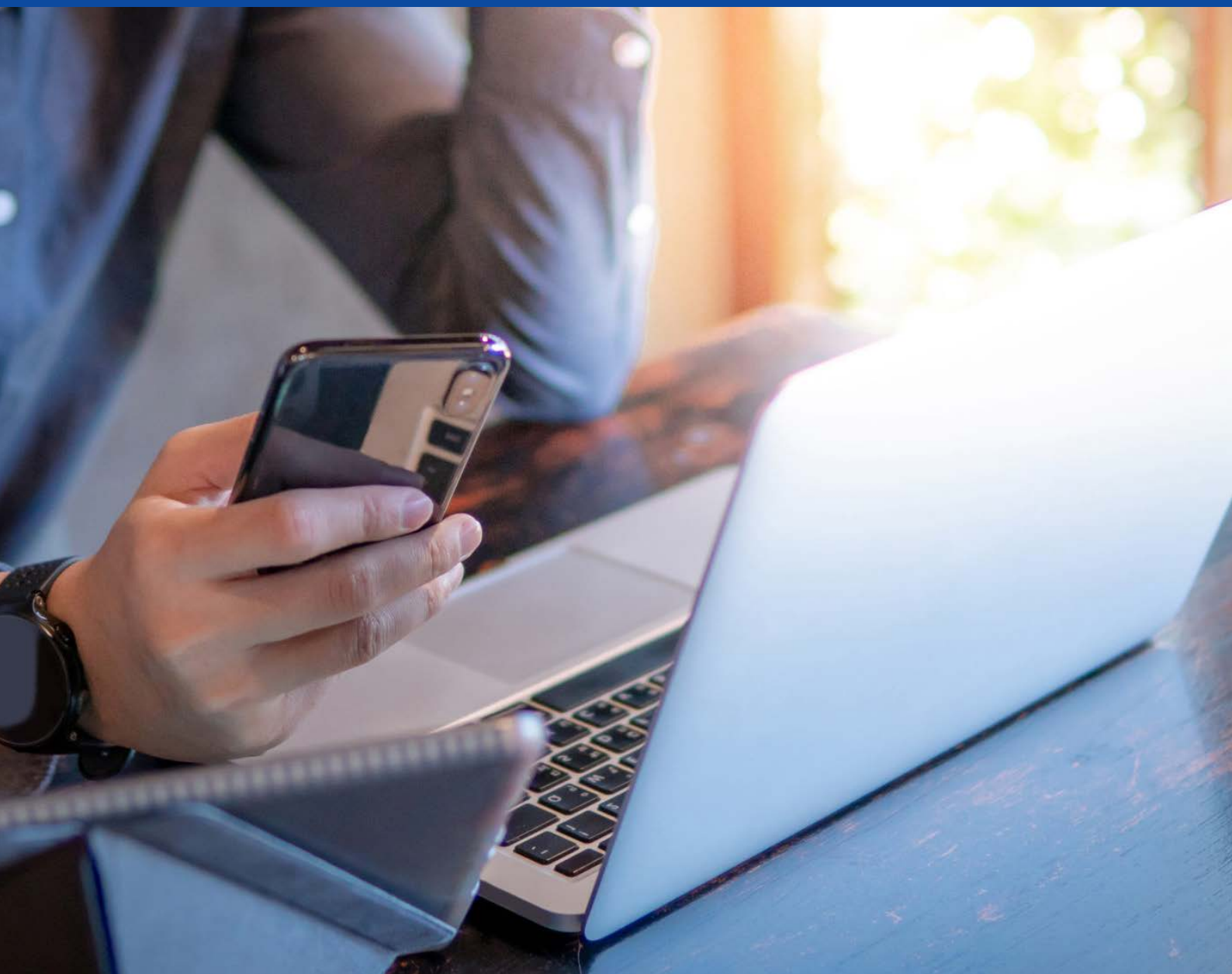
Information for customers on the Contingent Reimbursement Model Code for APP scams (the CRM Code)

This guide explains how the CRM Code for Authorised Push Payment Scams works



Sections

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. Early engagement with your bank will benefit any investigation and/or tracing of funds, 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 or by clicking here

If you have been a victim of a scam and are finding it hard to recover from the experience, contact Victim Support on 0808 1689 111 or by clicking here

What is the CRM Code?

The CRM Code has been in place since May 2019 and applies to Payment Service Providers.[1] It provides 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.

You can find a full list of signatory firms on the LSB website

Have you been a victim of an Authorised Push Payment scam?

Authorised Push Payment scams (or APP scams) occur when 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 CRM 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.

There are many different kinds of APP scams, including:

- **Safe account** - fraudsters convince people to move money to another bank account, to protect against fraud
- **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
- **Purchase scams** – sending money to buy goods that don't exist or are not as advertised
- **Invoice scams** – where fraudsters send a false invoice, often pretending to be from a company that the victim is expecting a bill from (e.g. HMRC)

1 Payments Service Providers include banks, building societies, credit unions, and electronic money and payments institutions. The term 'bank' will be used throughout this guide for simplicity, but it also includes these other payment services providers, as they may be involved in transferring your money.

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

Where the Code does not apply

- ✖ Where someone takes money from your account without your permission
- ✖ Where 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)
- ✖ Where payments are made using cash, cheque, credit, debit or prepaid card

You can find out more about your rights, unauthorised scams and credit/debit/prepaid card fraud from the Citizen's Advice Consumer Service: 03454 04 05 06 or here

What do banks who sign up to the Code do to protect me?

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 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 also agree to reimburse customers who have lost money to APP scams in some circumstances

How can I protect myself?

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.**

Here are some of the things you could do to protect yourself when making payments from your bank account:

- 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*
- 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
- When making a payment to an individual or organisation, take a moment to consider whether:
    - The person you're paying is who you were expecting to
    - The payment is for genuine goods or services
    - The person or business you are paying is legitimate

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, it 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.

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

01

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 it is important to get in touch with your bank as soon as possible. It will also benefit any investigation your bank may wish to conduct. You may also wish to contact the police, but contacting your bank is the first priority.

02

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.

03

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.

04

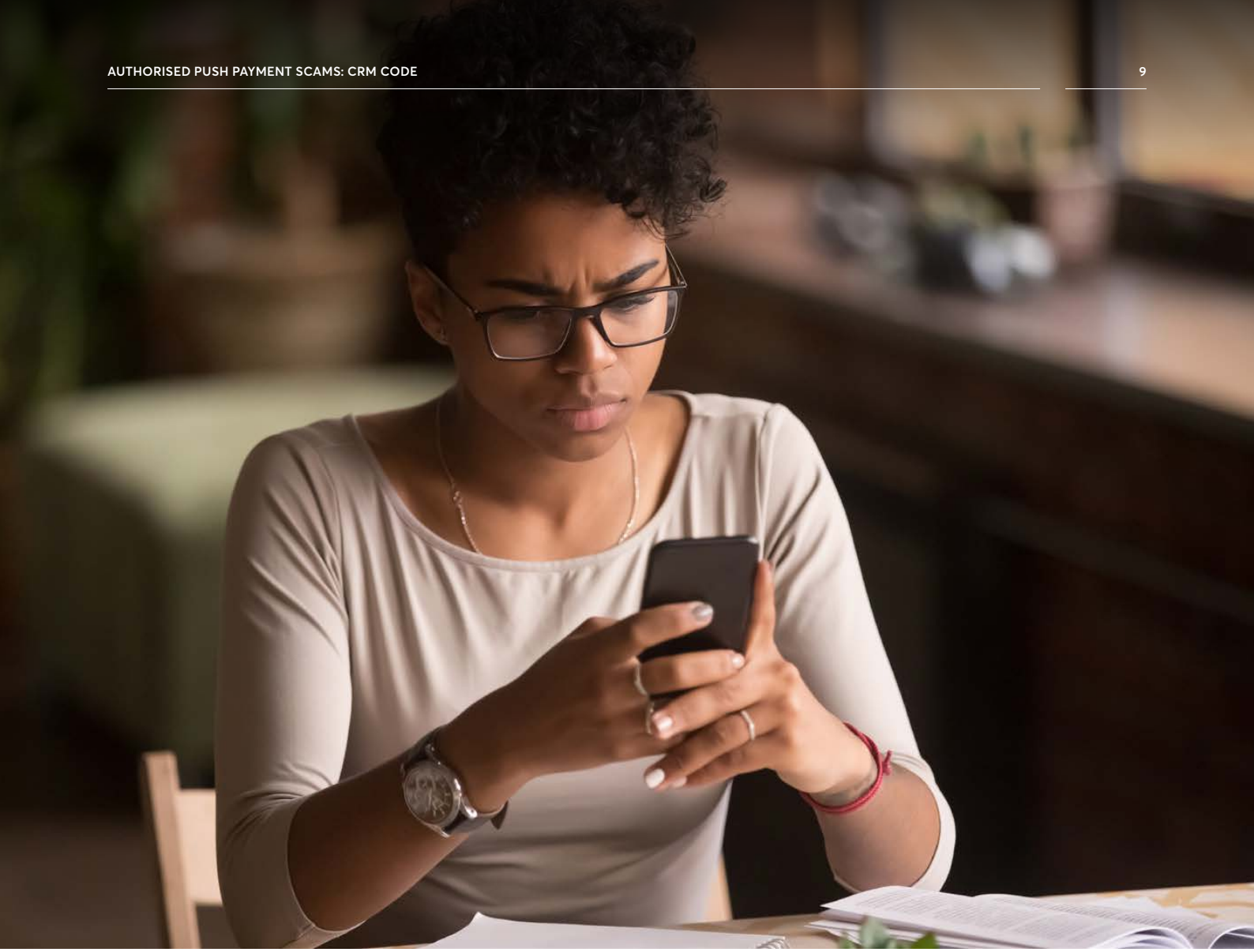
If your bank is a signatory to the Code then you should ask your bank to investigate whether you are entitled to get your money back under the Code.

The bank should normally let you know within 15 business days (or 35 days in extraordinary circumstances). If your bank is not a signatory, then you can still ask your bank to investigate.

Raising a complaint

If your bank has decided not to reimburse your funds, or only to reimburse a portion of the funds lost, you can raise a complaint. Your bank will provide information on how to raise a complaint to both your bank and the receiving bank (the bank to which the funds were sent), and the process to follow should you wish to do so. Always contact your bank in the first instance.

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 here or call 0800 023 4567.



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 taken the steps set out above to protect yourself.

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 steps outlined you may not get any money back, although a bank might choose to make a goodwill payment.

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:

Which?

Website

Money Helper

Website or

0800 138 7777

Citizen's Advice Consumer Service

Website or

03454 04 05 06

Age UK

Website or

0800 678 1602

Victim Support

Website or

0808 1689 111