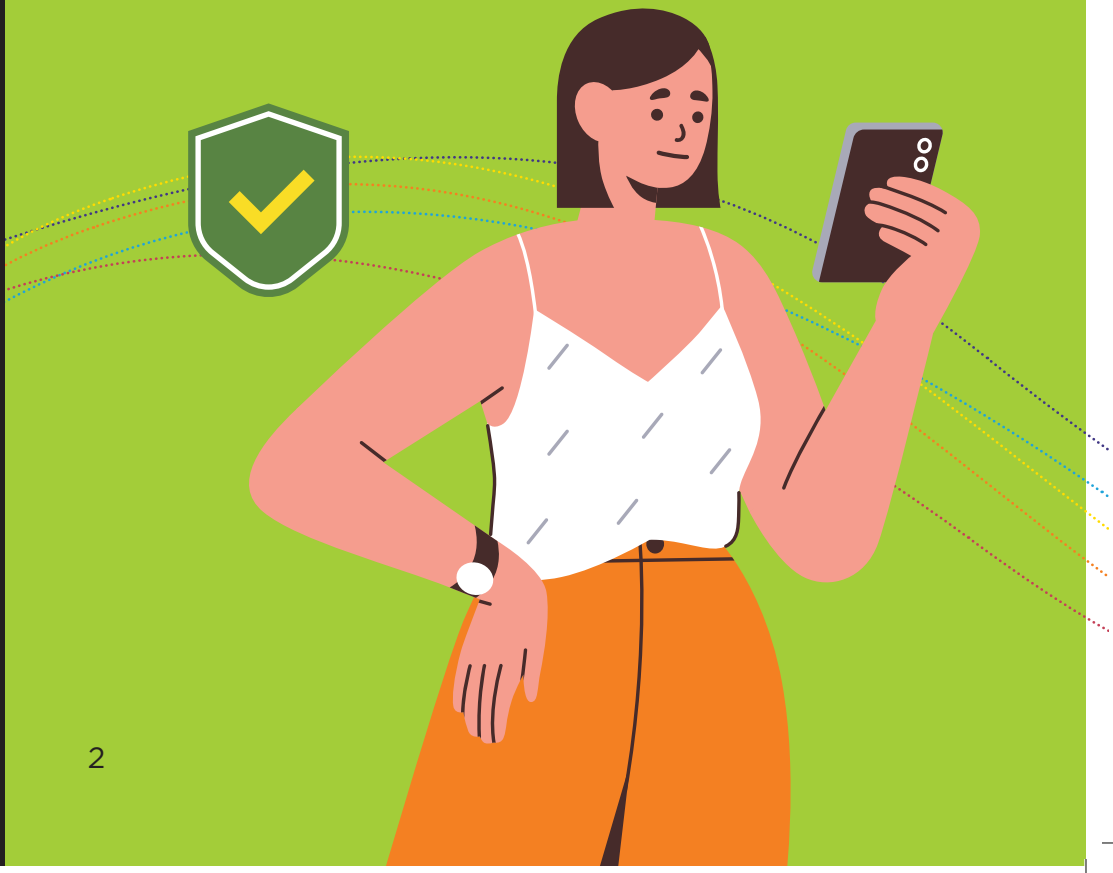
Your guide to

Authorised Push Payment Fraud Reimbursement

TAKE FIVE TO STOP FRAUD™

1. Introduction

This is a guide to the rules on how banks and other payment service providers reimburse victims of authorised push payment fraud. These rules have been set by the Payment Systems Regulator (PSR), the body that regulates payment systems in the UK.

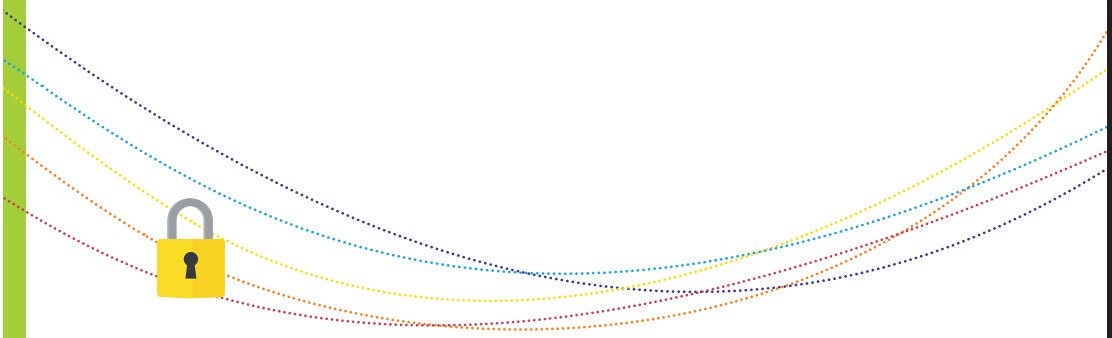


Throughout this guide we have used the word 'bank' for ease, however the rules apply to all payment services providers, such as building societies, e-money organisations, and fintechs.

These rules only apply to payments made on, or after, 7 October 2024.

You should still take care when you make a bank payment. Reimbursement is not guaranteed in all cases, with some specific exemptions applied. There's more information about how to protect yourself against authorised push payment fraud towards the end of this guide.

There is also a glossary at the end which explains what some of the terms used in the guide mean.



2. What is authorised push payment (APP) fraud?

Authorised push payment fraud happens when you are tricked by a criminal into sending money by bank payment to an account that they control and which you do not.

You can make a bank payment through online and mobile banking, at your branch or by telephone banking.

Every year thousands of people and businesses are victims of APP fraud. Common types of APP fraud include:

- **purchase fraud**, where criminals pretend to sell things that don't exist.
- **impersonation fraud**, where criminals claim to be someone from a bank, the police or another trusted organisation to steal money.
- **investment fraud**, where you're convinced to move your money into a fictitious fund or to pay for what later turns out to be a fake investment.
- **romance fraud**, when criminals use a fake dating profile to start a relationship with you and then ask for money.
- **invoice fraud**, where fraudsters send false invoices.

If a payment is taken from your account by someone else without your permission, it is called unauthorised fraud. For example, if your bank card is stolen and used to buy something in a shop or online. There are separate rules for reimbursing unauthorised fraud, including credit and debit card fraud, and you should seek advice in this instance. Contact your bank immediately if you spot any transactions that you do not recognise.

Remember, fraud affects people from all walks of life, and you should never be embarrassed if you have been scammed. Your bank will be there to help you.

3. What the rules cover

Covered:

- ✓ **Payments made within the UK. You are not covered for a payment sent overseas.**
- ✓ **Payments made using Faster Payments.**
- ✓ **Payments made using CHAPS.**
- ✓ **Payments from personal bank accounts and payments made by micro-enterprises and certain charities.**

Your bank may have different rules and processes if you are sending money within the same organisation. They will make you aware of this if the rules are different.

Not covered:

There are some situations where you won't be able to get your money back under this reimbursement scheme. This includes if:

- **You paid using cash, a cheque, or a credit, debit, or prepaid card.**
- **You paid using a payment system not covered under this scheme.**
- **It's a civil dispute: for example, if you've paid a genuine retailer or business but you aren't satisfied with the product or service you've received.**
- **You have acted fraudulently yourself – including if you have lied or misrepresented your circumstances for financial gain.**
- **It's a payment you have made to another account that you control.**
- **The payment you made is unlawful: for example, if the payment was for an illegal item.**
- **It is a payment to and from an account with a credit union, municipal bank, or a national savings bank (state-owned savings bank in the UK).**

Remember, you may have reimbursement options under other rules, so always seek advice.

4. The Consumer Standard of Caution

You should always be careful and cautious when making payments. This means meeting the Consumer Standard of Caution:

- **You need to follow any advice or warnings provided by your bank and law enforcement. This may include advice on how to check that your payment is genuine, or an alert to advise that they think it may be fraud. Your bank and law enforcement will never ask you to transfer money to protect yourself from fraud.**
- **You must report the fraud as soon as you can, and no more than 13 months after the last fraudulent payment was made.**
- **Your bank may ask you for additional information about your claim. You need to make sure you respond to these requests.**
- **Once you have made a claim, your bank may ask you to report the details of the fraud to the police, or they may offer to do this on your behalf. You should consent to these steps being taken where possible and reasonable.**

Your bank does not have to reimburse money lost in an APP fraud if you have shown a significant degree of carelessness (known as 'gross negligence') when making a payment. This would mean you would not have met the Consumer Standard of Caution.

5. What should I do if I think I have been scammed?

Contact your bank immediately if you have lost money in an APP fraud. It is important that you do this as soon as you realise that you may have been scammed as delays can cause problems when trying to recover your funds.

You must report the fraud no more than 13 months after the last fraudulent payment was made.

The maximum amount of money you can claim under the rules is £85,000.

Your bank may ask you for information or documents to help with your claim. This could include messages or screenshots. You should give them your consent to share information about your case with other banks where necessary.

You should co-operate fully with your bank when it comes to involving the police. They will help and advise you on how to do this based on their own ways of working.

6. How long will it take to be reimbursed?

Every claim will be assessed on a case-by-case basis. As part of the process your bank will consider the evidence presented by you, any service providers involved and – where relevant – a third party, such as the police.

If your claim is valid, in most cases you should be reimbursed within five business days of making a claim. Business days are Monday to Friday, excluding Bank Holidays.

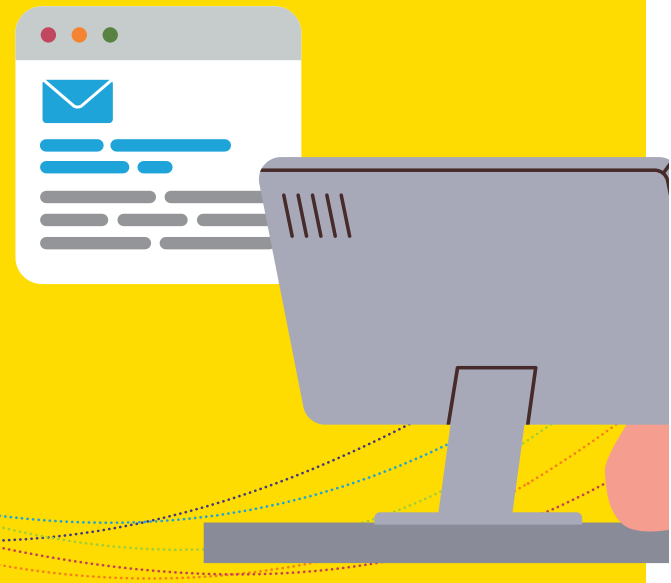
In some cases it can take up to 35 business days to be reimbursed. This is when your bank needs extra time to gather information from you, the bank that received the payment, or a statutory body (such as the Financial Conduct Authority) to inform their assessment of the case.

An excess of up to £100 may be deducted from any money that is reimbursed. Your bank may choose a different excess up to the maximum of £100, or not apply any excess at all. Your bank will confirm the exact amount and how this will be applied.

7. What happens if I am a vulnerable customer?

There are additional protections in place for customers who, due to their personal circumstances, may be more vulnerable to being tricked by criminals. This can include a health condition, or a life event such as a bereavement.

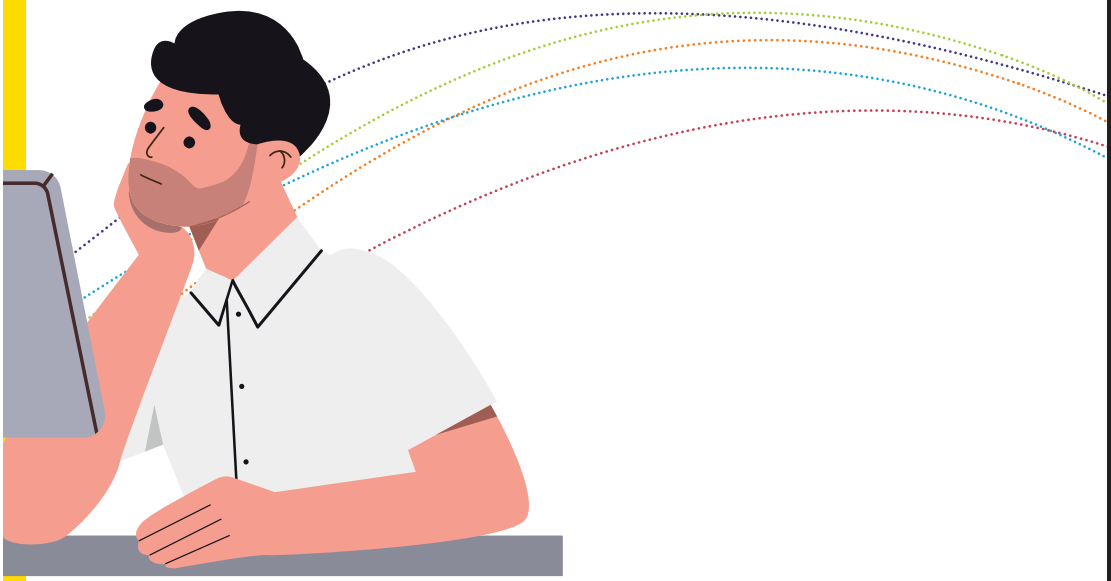
It could also include personal factors, such as your knowledge of financial matters, your personal financial situation, your ability to withstand an emotional shock or your levels of capability – such as literacy or digital skills.



If these circumstances have had an impact on your ability to spot or protect yourself from fraud, then you can still be reimbursed even if you did not take all the steps required under the Consumer Standard of Caution.

Your bank will also consider your personal financial circumstances when deciding how – or if - to apply an excess to your reimbursement.

If you are a vulnerable customer there will be no excess applied.



8. Where can I go for more support?

Your bank should be your first point of contact – and you should use a number for them you know to be genuine, such as the one on the back of your card. You should also report fraud to Action Fraud, the national fraud and cybercrime reporting centre for the police. You can contact Action Fraud on **0300 123 2040** or at **www.actionfraud.police.uk**.

If you are in Scotland, please report it to Police Scotland directly by calling **101**.

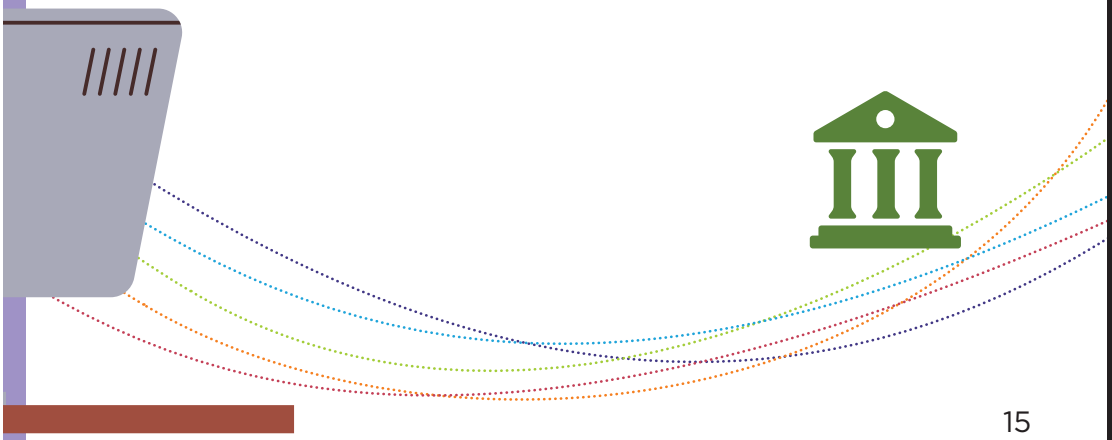
If you have a complaint about your bank, you should contact them directly. If they cannot deal with your complaint by the day after they receive it, they will contact you to let you know they are looking into it. They must tell you about their progress.

If you're not happy with the outcome of your complaint, you can contact the Financial Ombudsman Service (FOS) which is independent and impartial. They will review your complaint by weighing up all the facts. This is a free service. For further information please visit **www.financial-ombudsman.org.uk**.

Being scammed can also be traumatic and upsetting, so be sure to ask for help and support if you need it.

If you have been a victim of fraud and are finding it hard to recover from the experience, you can find further support via:

- Age UK
- Citizen's Advice Consumer Service
- Victim Support



9. How to protect yourself from APP fraud

Criminals are experts at impersonating people, organisations, and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment. Stop and think. It could protect you and your money.

Before making a payment, follow the advice from Take Five to Stop Fraud:

- Take a moment to **stop and think** before parting with your money or personal information. It could keep you safe.
- **Ask yourself, could it be fake?** It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Do your research** and be suspicious of any too-good-to-be-true offers or prices.
- **Remember**, your bank or the police will never ask you to transfer money to a safe account.
- If you're unsure or are suspicious then talk to a trusted friend or family member before making your payment.

For more information visit
www.takefive-stopfraud.org.uk/app-guide

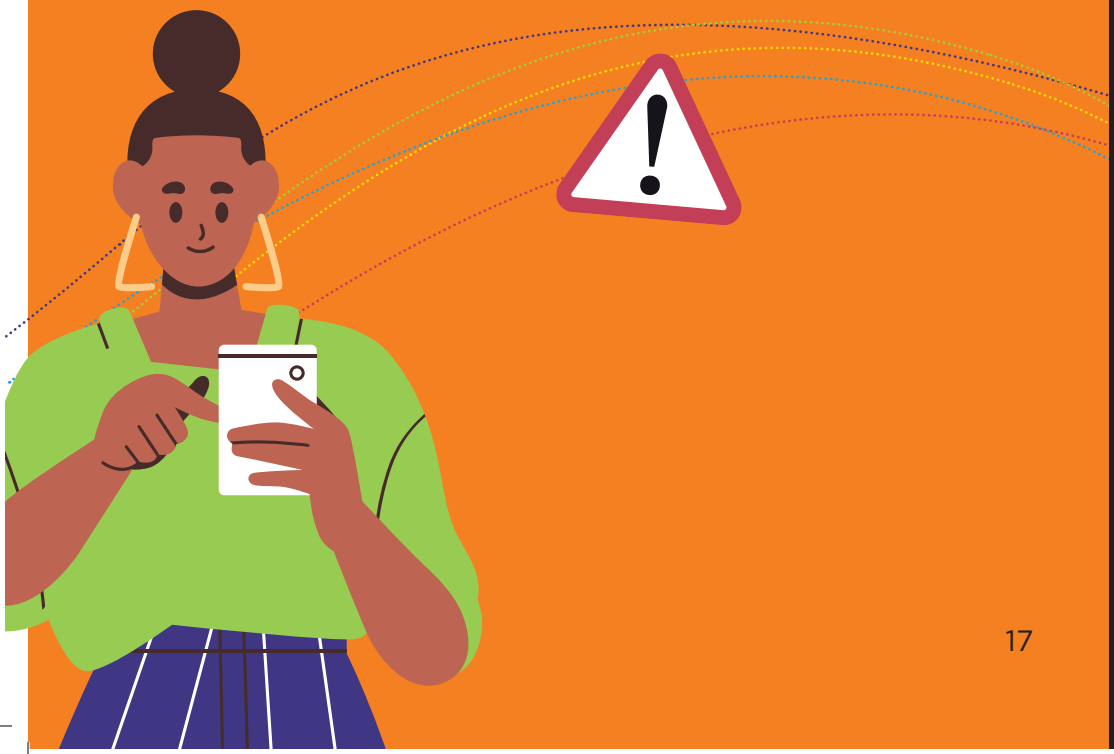
TAKE FIVE TO STOP FRAUD™

When you are making a payment:

Always follow any advice or warnings from your bank or payment service provider.

Your bank might ask you extra questions about a payment. This is to help keep you safe. Always answer these questions truthfully. If someone is asking you to lie or telling you what to say to your bank, then it's very likely to be a scam.

It might take slightly longer for a payment to leave your account. This is so your bank has time to do extra checks to keep you safe from fraud.



Glossary

Building Society

A customer-owned financial organisation that provides services including savings, mortgages and other lending.

CHAPS

CHAPS (Clearing House Automated Payment System) is a payment method used to transfer large amounts of money. CHAPS is commonly used by solicitors and conveyancers to complete housing and other property transactions. Individuals may use CHAPS to buy high-value items such as a car or pay a deposit for a house.

Certain Charities

Charities covered by these reimbursement rules have an annual income of less than £1 million.

Credit Unions

A financial co-operative that is owned and controlled by its members, providing members with services including savings and lending.

E-money organisation

A financial organisation that is authorised to issue or redeem electronic money - cash or money in digital form.

Faster Payments

A quick way of sending money between bank accounts.

Financial Conduct Authority

The organisation that regulates financial services in the UK.

Fintechs

A financial organisation that uses financial technology to provide products and services to customers.

Micro-enterprises

A micro-enterprise is a business that employs fewer than ten persons and whose annual turnover and/or annual balance sheet total does not exceed €2 million.

Payment service provider

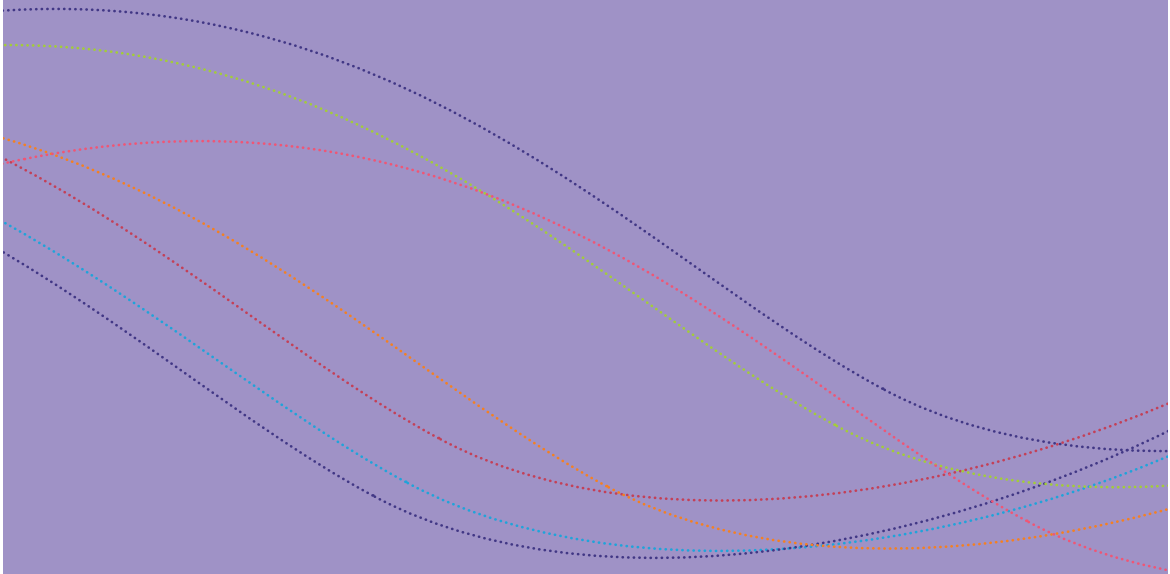
A third party company that facilitates electronic payments.

Statutory body

An organisation that can check the activities of a business or organisation are legal and follow the rules.

Vulnerable customer

Someone who, due to their personal circumstances, is especially susceptible to harm. This could include a health condition, a life event such as a bereavement, low resilience to financial or emotional shocks, and low capability, such as poor literacy or numeracy skills.



TAKE FIVE TO STOP FRAUD™

UK Finance

 | Version 1 October 2024