The new APP (authorised push payment) fraud reimbursement scheme

The APP (authorised push payment) fraud reimbursement scheme will apply from 7th October.

The following aims to provide you with information on APP fraud and the new scheme. If you fall victim to an Authorised Push Payment (APP) fraud, you have the right to be reimbursed under certain conditions. It's important to understand your rights, the scope of the reimbursement process, and what is required from you.

What is APP (authorised push payment) fraud?

APP fraud means an 'authorised push payment' fraud whereby a customer is tricked into sending funds to a fraudster who has posed as a genuine payee

Please be aware of APP fraud scam types:

- **Purchase Scams - on** social media platforms, scammers pose as sellers offering non-existent, *'too good to be true'* offers like tickets, clothing, or vehicles, asking for payment via bank transfer
- **Investment Scams -** the promotion of fake investment opportunities, with promises of high returns and low risk. Professional-looking websites or direct contact; scammers impersonate legitimate investment firms or falsely claim celebrity endorsements
- **Romance Scams -** on dating sites or social media, scammers create fake profiles to build relationships and then request money under false pretences, preying on victims' emotions
- **Advance Fee Scams -** scammers ask you to pay an upfront fee for a service that is never provided, such as a loan, lottery win, or in connection with a job offer
- **Invoice and Mandate Scams -** scammers will send emails or hack into email systems to pose as legitimate companies, redirecting payments to fraudulent accounts.
- **CEO Scams -** scammers impersonate senior executives within a business, pressuring employees to make urgent payments to fraudulent accounts
- **Impersonation Scams: Police/Bank Staff/Tech support/friends & family or other -** scammers impersonate legitimate individuals, companies or loved ones to pressure you into making urgent payments to fraudulent accounts. Fraudsters may pose as a government official, tech support agent, or someone the victim may think they know or trust i.e. Police/Bank Staff

What Payments are in Scope?

You will be eligible for reimbursement if the payment you made meets the following criteria:

- **Who Can Be Reimbursed:** Individuals, microenterprises, and charities are eligible.
- **Type of Payment:** The payment must be made using Faster Payments or CHAPS in the UK.
- **Where the Payment Was Sent:** The payment must be sent to a UK account that you, as the payer, do not control.
- **Conditions for Reimbursement:**
    - The payment was authorised by you but did not go to the intended recipient, or
    - The payment was made for a different purpose than you intended.

What You Need to Know and Do

Protect yourself and report concerns immediately. You should:

1. Follow Guidance: Pay attention to any warnings about different types of scams and recommendations relating to specific payments, taking precautions where required.

2. Report Scams Promptly: As soon as you suspect or become aware of a scam, report it to us immediately - we may be able to freeze funds or request other companies to do so.

3. Provide Necessary Information: You need to provide details about what happened, promptly. This information is vital for processing your claim.

4. Cooperate with Law Enforcement: Report the scam to the police or consent for us to do so on your behalf, as this supports the investigation and your claim.

By adhering to these steps, you help ensure a smooth reimbursement process.

Time limits

● Reimbursement applies only to payments made on or after 7 October 2024.

● Claims must be raised within 13 months of the final payment made to the fraudster as part of the same scam.

Claim excess

A maximum excess value of £100 may apply to the reimbursable APP scam claim.

Maximum claim limit

The maximum level of reimbursement is £85,000.

Vulnerable Customers

We understand that some customers may be more vulnerable than others. When making a claim, please let us know if you consider yourself to be a vulnerable customer and how this vulnerability affected your ability to protect yourself from the scam.

Exclusions to the reimbursement requirement

● **First party fraud**

● **Gross negligence:** if the consumer standard of caution was neglected

● **Time exclusions:** (e.g., claims made before 7 October 2024 and APP claims submitted more than 13 months after the final payment to the fraudster)

● **International payments:** Payments made outside the UK.

● **Payments Using Other Systems:** Payments that occur across other payment systems, or using cheques or cash.

● **Unauthorised Payments:** Payments made to an account you control, or that were not authorised by you.

● **Civil disputes**

● **Payments Involving Certain Institutions:** Payments sent or received by credit unions, municipal banks, or national savings banks.

● **On-Us Payments:** Payments made between accounts within the same financial institution.

How to raise a claim

To raise a claim, you can contact us at the following address:

APP-fraud-claims@lerextech.com

● The assessment of your scam claim should generally be completed within 5 business days

● If additional information is required from you or other involved Payment Service Providers, the timeframe may be extended, but the final assessment will be completed within 35 business days from the date the claim is raised.

● You will be informed and updated if the timeframe is extended.

If you are dissatisfied with the outcome of your claim, you may follow the existing complaint process or escalate the matter to the Financial Ombudsman Service (FOS).

When raising a claim for an APP scam, it's important to include the following details to ensure your claim is processed efficiently:

Information to Include in Your Claim

1. Account information:

● Provide the sort code and account number of the account from which the payment(s) was made.

● Provide the sort code and account(s) number of the account to which the payment(s) was sent.

2. Amount of the scam: Please include the amount of all APP scam payments.

3. Scam Description: Clearly explain what happened, including who you believed you were paying and why you made the payment. Describe how you were deceived and the circumstances leading to the scam.

4. Payment Purpose: State the intended purpose of the payment, such as buying goods or investing in a scheme, or other purposes.

5. Communication with the Scammer: Provide details on any ongoing communication with the scammer, including whether you're still in contact.

6. Supporting Evidence: Include any documentation that supports your claim, such as emails, messages, screenshots, or transaction confirmations, which demonstrate that the payment was not intended for the recipient it ultimately reached.

7. Any additional information.

By providing this information, your claim can be accurately assessed and it will increase the likelihood of a favourable outcome.

What are we doing to protect you?

- Our aim is to educate you on how to both spot and stop APP frauds. We will send you helpful information and you will find information on our website.
- We are updating the terms and conditions to ensure that your rights are protected.
- We have introduced fraud warnings, to stop and make you consider the risks before sending a payment to someone new, or changing the payment details for an existing company or person.
- When adding new payment details the system will validate that the name and account details match, adding an extra layer of protection.
- If you feel that you have been the victim of an APP fraud scam, please use the information in this document to help to determine if you have a valid claim under the scheme and use the details provided to make a claim.

How can I protect myself?

Be aware of APP fraud scams and how to avoid them:

- If you do not know the recipient or are not sure the recipient is genuine, you should not proceed with the payment.
- Be aware that fraudsters often impersonate the police, financial institutions, governmental institutions or loved ones.
- Check the legitimacy of whomever is asking you for payment by contacting them on a number that you sourced independently.

Ask yourself:

- Is this an unexpected payment?
- Is this an unexpected change of payment details?
- Am I being pressured to make this payment?
- Am I sure the person requesting it is who he/she claims to be?
- Am I confident that the 'too good to be true' offer is real and that I will receive the goods or service?

Help from other organisations

● Police.uk - Reporting a crime to the Police - https://www.police.uk/

● FCA's ScamSmart - Check potential investment or pension deals to make sure they're legit - https://www.fca.org.uk/scamsmart

● Victim Support - Support for victims and guidance on types of fraud -

https://www.victimsupport.org.uk/

● Action Fraud - Reporting crimes and info about how to protect yourself -

https://www.actionfraud.police.uk/

● TakeFive - Advice on the avoidance of scams - https://www.takefive-stopfraud.org.uk/

● Age UK - Information on how to spot and avoid scams - https://www.ageuk.org.uk/