Emerald Financial Group (UK) LTD
Hamilton House, 1 Temple Avenue,
London EC4Y 0HA, United Kingdom.
https://emerald24.co.uk
hello@emerald24.co.uk

APP Scams: Reimbursement Rules

To submit an APP Scam reimbursement claim to Emerald24, please send a message via your Emerald24 mobile app or Emerald24 online portal. Before completing the form, please ensure you have read the below information, as only claims that meet all regulatory requirements will be approved.

The Payment Systems Regulator (PSR) has announced the introduction of new reimbursement rules for eligible victims of authorised push payment scams (APP Scam Reimbursement Rules). These rules will come into force on 7 October 2024.

Under the APP Scam Reimbursement Rules, if you are a consumer, micro-enterprise or charity and have been the victim of an authorised push payment scam (APP Scam) from 7 October onwards, you may be able to submit a reimbursement claim to your payment service provider up to a value of £85,000.

We've set out below further information regarding eligibility criteria, circumstances when a claim may not be approved and how to submit a claim to Emerald24.

What is an APP Scam?

APP Scams, also known as bank transfer scams, are a type of fraud in which an individual or organisation is tricked into transferring money to a fraudster's account. This type of fraud typically occurs when the fraudster poses as a legitimate individual or entity (such as a vendor, supplier, or employee of a company) or even family and friends.

The fraudster will usually contact the victim through email, phone, or text message and provide them with false information, such as fake invoices or payment requests. The victim is then instructed to make a payment to the fraudster's account, often under the guise of urgent or time-sensitive circumstances.

The fraudster will use various tactics to convince the victim to transfer the funds, such as creating a sense of urgency, threatening legal action or penalties, or providing fake assurances of security or legitimacy.

Once the victim transfers the funds, the fraudster will quickly withdraw the money from the account, often leaving the victim with little to no recourse to recover the lost funds.

Emerald Financial Group (UK) LTD
Hamilton House, 1 Temple Avenue,
London EC4Y 0HA, United Kingdom.
https://emerald24.co.uk
hello@emerald24.co.uk

Can I submit a reimbursement claim to you if I have been the victim of an APP Scam?

If you have been the victim of an APP Scam from 7 October 2024, you may be able to submit a reimbursement claim to us if the following has occurred:

- you are a consumer, micro-enterprise or charity;
  - "consumer" means an individual who, in contracts for payment services to which the Electronic Money Regulations 2011 and Payment Services Regulations 2017 apply, is acting for purposes other than a trade, business or profession
  - "micro-enterprise" means an enterprise that employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed €2 million (or equivalent)
  - "charity" means a body whose annual income is less than £1 million and is registered in accordance with the relevant legislation in the UK
- you are a customer of ours and hold an account with us;
- the payment transaction was authorised by you from your account held with us to a third party in the UK;
- the third party account that the payment was sent to is not controlled by you;
- the payment transaction was authorised on 7 October 2024 or later;
- the payment was sent in GBP as a Faster Payment or CHAPS Payment;
- the payment was sent to an unintended recipient that you were deceived into transferring to, or it was sent to the recipient after being deceived as to the purpose of the transfer; and
- the payment transaction was authorised within 13 months of the date you are making a claim.

If your claim meets the requirements set out above and no exceptions under the APP Scam Reimbursement Rules apply, then the final reimbursable amount (as determined by our investigation) will be paid to you within five (5) business days of receiving the claim (unless we are permitted to extend this timeframe under the APP Scam Reimbursement Rules).

Please note that an excess of up to £100 will be applied to an APP Scam claim if you are not a vulnerable customer. This amount will be deducted from the amount reimbursed to you.

Can my reimbursement claim be rejected?

Your APP Scam claim may not be approved by us in the following circumstances:

- if it did not meet the requirements set out above in 'Can I submit a reimbursement claim to you if I have been the victim of an APP Scam?'

Emerald Financial Group (UK) LTD
Hamilton House, 1 Temple Avenue,
London EC4Y 0HA, United Kingdom.
https://emerald24.co.uk
hello@emerald24.co.uk

- for any amount claimed in excess of £85,000;
- in respect of any international payments or payments made using cheques or cash;
- where payments are sent or received by credit unions, municipal banks and national savings banks;
- if the transaction is in a currency other than GBP or is a foreign exchange trade;
- if the consumer standard of caution exception applies (unless you are considered a vulnerable customer) – please see below section 'What is the consumer standard of caution exception?';
- if the amount claimed is the subject of a civil dispute or other civil legal action;
- if you have acted fraudulently, such as by committing first party fraud;
- if the APP Scam claim has been submitted fraudulently or dishonestly; or
- if otherwise required by applicable laws, including the APP Scam Reimbursement Rules set out by the PSR, Pay.UK and any other relevant regulatory authorities (as they may be amended from time to time).

Please note that the above list is a non-exhaustive list of the reasons your APP Scam claim may not be approved. We must assess your APP Scam claim on a case-by-case basis in accordance with the relevant APP Scam regulations and will only approve a claim that meets all regulatory requirements.

What is the consumer standard of caution exception?

The consumer standard of caution is a set of requirements which all customers are expected to meet. If any component is not met due to the customer's gross negligence, then an exception will apply and a payment service provider will be entitled to reject an APP Scam reimbursement claim.

Under the consumer standard of caution, customers are expected to meet the following requirements:

- to have regard to any specific interventions, such as warnings, given by their payment service provider or competent national authority (such as the police);
- to promptly report the scam to their payment service provider upon learning or suspecting of falling victim to a scam;
- to comply with appropriate information requests from their payment service provider to support the assessment of the claim; and
- to report to the police or allow their payment service provider to do so on their behalf, if required.

Where the victim was a vulnerable customer at the time the payment transaction was authorised, the consumer standard of caution exception will not apply.

Emerald Financial Group (UK) LTD
Hamilton House, 1 Temple Avenue,
London EC4Y 0HA, United Kingdom.
https://emerald24.co.uk
hello@emerald24.co.uk

How do I make an APP Scam claim?

From 7 October 2024, customers with eligible APP Scam claims (being claims that meet all of the requirements set out above) will be able to report them via Emerald24 mobile app or Emerald24 online portal. Please note that in order to investigate an APP Scam claim, we may be required to share personal information (such as your name and account information) with the receiving payment service provider.

To submit an APP Scam reimbursement claim to Emerald24, please send a message using your Emerald24 mobile app or Emerald24 online portal.

How can I protect myself against APP Scams?

We recommend customers try to take proactive steps to protect themselves against APP Scams, such as those listed below.

- Be wary of skeptical or unsolicited offers (such as investment opportunities that seem too good to be true) or payment requests. Make sure to research the company/individual first and don't be afraid to verify their identity by contacting them directly through their official contact details.
- If you have received an unexpected call or message from an organisation, verify that it is genuine by contacting the organisation directly through their official contact details.
- If someone is pressuring you to make a payment quickly, take the time to think about it before authorising any payments to them.
- Report suspected scams to relevant national authorities as soon as possible. Other helpful resources can be found at: Stop Scams UK.

What other types of fraud should I be aware of?

Account takeover

Account takeover is a type of fraud where criminals gain unauthorised access to a customer's account, typically through phishing scams, social engineering, or various forms of hacking to trick the account holder into providing sensitive information.

Once a criminal has access to an account, they can steal funds, make unauthorised transactions, or change the account details to lock the legitimate owner out of their account, causing significant financial losses.

Emerald Financial Group (UK) LTD
Hamilton House, 1 Temple Avenue,
London EC4Y 0HA, United Kingdom.
https://emerald24.co.uk
hello@emerald24.co.uk

Preventative measures include implementing strong authentication measures and security protocols such as multi-factor authentication, monitoring for suspicious login activity, educating customers, and having a response plan and a refined procedure in place for notifying affected customers and law enforcement agencies.

Cyber fraud

Cyber fraud refers to any fraudulent activity that takes place online and typically involves using the internet or technology to deceive individuals and organisations into providing sensitive information.

It includes phishing scams, identity theft, hacking, and malware attacks. Cyber fraud can be committed by individuals or organised groups who target vulnerable entities lacking adequate security measures.

Examples include email scams requesting, fake websites, and ransomware attacks, leading to financial loss, reputational harm, and legal consequences.

To prevent cyber fraud, keep software up to date, use strong and unique passwords, be wary of suspicious emails and messages, use two-factor authentication and keep sensitive information private.

CEO email fraud

CEO email fraud, also known as business email compromise, is a type of cyber fraud where criminals impersonate a CEO or another high-level executive to trick employees and partners into transferring funds or sensitive information, causing significant financial losses and reputational damage.

The fraudster creates an email address similar to the targeted executive's by slightly altering the domain name, then requests urgent payment or transfer from the finance or accounting department, and uses various tactics to create a sense of urgency or authority by claiming the requested funds are needed to close a critical deal. The funds will then be sent to the criminal's account through a series of intermediaries or shell accounts. These are often difficult to trace.

To prevent this fraud, payment firms should implement strict authentication protocols for all financial transactions including multiple levels of approval, educate employees, conduct regular security audits, and have a response plan in place for recovery of stolen funds and notifying law enforcement.