punjab national bank (International) Limited

We are all susceptible to fraud. Stay Vigilant, Stay Safe.

From the 7th day of October 2024 new rules mean that if You are an eligible Authorised Push Payment (APP) Scam Victim, You may be entitled to a refund of an eligible APP Scam Payment made from Your Account with us up to a maximum Reimbursable Amount specified by the regulator.

The regulator has specified eligible APP Scam Payments (as Faster Payments or CHAPS payments) and an App Scam Reimbursable Amount (currently £85,000). This may change at any time.

We are permitted to charge a Claim Excess up to a maximum amount specified by the regulator (currently £100) for each separate APP Scam Claim. We'll take your personal circumstances into account and where they have a material impact on your ability to protect yourself from the scam, the excess will not apply.

What is an APP Scam?

A person uses a fraudulent or dishonest act or course of conduct to manipulate, deceive or persuade You into transferring funds from Your Account with us to an account in the UK that You do not control when,

You meant to send money to someone else, but You were deceived into sending it to another person.

You sent money to someone for what You thought was a genuine reason, but it turned out to be a scam.

What is an eligible APP Scam Payment?

This is a domestic faster payment or a CHAPS payment made from Your Account to the instructed account in the UK which You do not control because of an APP Scam where,

(1) the payment is not to the intended recipient, or, the payment is not for the purpose that You intended, and
(2) the payment is not the subject of a civil dispute or other civil legal action, and
(3) the payment was not made for an unlawful purpose.

Other types of payments e.g., international payments, cash withdrawals, payment by cheque, payment by debit card, credit card or loan payments are not eligible APP Scam Payments.

Are You an eligible APP Scam Victim

(1) You are an individual and have a personal account with us, or,
(2) You have a business account with us and (You employ less than ten persons and have an annual turnover or annual balance sheet not exceeding £2Mn or You are a charity with an annual income of less than £1Mn).
(3) You have reported that an APP Scam payment has happened in your Account ***on or after the 7th day of October 2024***.
(4) You tell us that You have been the victim of an App Scam and make an APP Scam Claim under the mandatory reimbursement rules within 13 months of the date of the final APP Scam Payment leaving Your Account.
(5) You are not a party to the fraud or dishonesty.
(6) You are not making a fraudulent or dishonest claim.

We will refund You up to the maximum Reimbursable Amount for each eligible APP Scam Payment. We will not pay You any more than the maximum Reimbursable Amount. We will provide You with an explanation if we do not refund the full APP Scam Payment.

We will usually refund an eligible APP Scam Payment within a period of five Working Days from our receipt of Your APP Scam Claim but Your payment may be delayed if,

(a) We have requested information from You and we are waiting for You to provide information which we need to assess Your APP Scam Claim or your status as a vulnerable customer, or
(b) We are waiting for information from the recipient bank to assess Your APP Scam Claim, or
(c) We have evidence of Your fraud and we are gathering information from the recipient bank, law enforcement or other relevant parties, or
(d) We become aware that there are multiple banks involved in the APP Scam Payments and we are gathering information from all recipient banks.

We will respond to Your APP Scam Claim within a maximum of five business days of receipt of the information that we have requested from You or others.

We will always respond to Your APP Scam Claim within a maximum of thirty-five Working Days of our receipt of Your APP Scam Claim.

You must pay attention to any warnings or guidance given by the bank for instance Fraud warning messages.

We may reject Your APP Scam Claim when You have failed to exercise the Consumer Standard of Caution because of gross negligence.

What is the Consumer Standard of Caution?

(a) You must pay attention to any intervention made by us or by the police or, the National Crime Agency or any other competent national authority named by the regulator.
(b) You must report the APP Scam Claim to us promptly upon learning or suspecting that You have fallen victim to an APP Scam. Call us on 0800 849 9229, send an email to customersupport@pnbint.com or visit one of our branches.

(c) You must respond to any reasonable and proportionate requests for information from us.
(d) After making an APP Scam Claim You must consent to us reporting to the police on your behalf or report the APP Scam claim directly to the police, National Crime Agency or any other competent authority named by the regulator at our request.

What happens if you are 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. If this has had an impact on your ability to spot a scam, you can still be reimbursed – even if you did not meet the Consumer Standard of Caution.

If Your APP Scam Claim is rejected we will tell You the reason for rejecting Your claim unless some legal, regulatory, or other reason prevents us from doing so or we believe that doing so would undermine our security measures.

If we do not deliver the standard of service You expect or if You think we have made a mistake please let us know. We will investigate the matter and if necessary set about putting things right as soon as possible.

If You feel that Your concerns have not been satisfactorily addressed by us You may refer the matter to the Financial Ombudsman Service (FOS). Complaining to the Financial Ombudsman does not affect Your legal rights. You can find more details on Financial Ombudsman Service website https://www.financial-ombudsman.org.uk

How to stay safe from different type of scams?

Scam Warning !: Buying Goods or paying for a service for e.g. bills, invoices or rent.

Could this be a Purchase scam?
In a purchase scam, the victim pays in advance for goods or services that are never received. These scams usually involve the victim using an online platform such as an auction website or social media.

How to stay safe from purchase scams:

- Be suspicious of any offers or prices that look too good to be true.
- Always use the secure payment method recommended by reputable online retailers and auction websites. Be very wary of requests to pay by bank transfer.
- Always do your research and ask questions before you buy. Ask to see any vehicle in person first and request the relevant documentation to ensure the seller owns it.
- If you're buying an item made by a major brand, you can often find a list of authorised sellers on their official website.
- Contact your Bank straightaway if you think you may have fallen for a purchase scam.

Scam Warning !: Making a large purchase for e.g. a car, property etc.

Could this be a Payment scam?
In a payment scam, the victim pays in advance for goods or services that are never received. These scams usually involve the victim using an online platform such as an auction website or social media.

How to stay safe from purchase scams:

- Be suspicious of any offers or prices that look too good to be true.
- Always use the secure payment method recommended by reputable online retailers and auction websites. Be very wary of requests to pay by bank transfer.
- Always do your research and ask questions before you buy. Ask to see any vehicle in person first and request the relevant documentation to ensure the seller owns it.
- If you're buying an item made by a major brand, you can often find a list of authorised sellers on their official website.
- Contact your Bank straightaway if you think you may have fallen for a purchase scam.

Scam Warning !: Paying to Family or Friends.

Could this be a Family/Friend scam? How well do you know this person? Take time to think.

We want to make it as easy as possible to pay the people you trust. If you met this person online and they've asked you to transfer money, stop and think before making your payment. Contact another member of your family you trust to confirm.

Scam Warning !: Paying to your other account.

Could this be a safe account scam? Have you been asked to make this payment unexpectedly?

We will never ask you to move your money.
Criminals often pose as your Bank, the Police or other Companies you trust to convince you to transfer your own money to a 'safe' account. Genuine organisations will never ask you to move your money to keep it safe. Stop and think.

Scam Warning !: Investment.

Could this be a scam? Are you feeling rushed into making this payment? Take time to think.

In an investment scam, a criminal convinces their victim to move their money to a fictitious fund or to pay for a fake investment. The criminal will usually promise a high return in order to entice their victim into making the transfer. These scams include investment in items such as gold, property, carbon credits, cryptocurrencies, land banks and wine.

If you are feeling pressured into making this payment or you've been asked to select this specific payment reason, then its highly likely to be a scam.

Seek advice when investing.
We strongly recommend that you seek independent advice and thoroughly research the firm online including a review of the FCA register which can be found on the FCA website. Some criminals may actually give you an initial return on your investment, only to convince you to make a larger payment. If you feel pressured into investing quickly, STOP and discuss with someone you trust. If you decide to proceed and the investment turns out to be a scam, you will lose your money.

Scam Warning !: Payment related to Crypto Currencies Investment.

Could this be a Crypto Currency /Investment scam?
If you've been contacted by a 'trader' promising big profits and offering to help you invest in cryptocurrency, this is a scam

Do you have control of the Cryptocurrency wallet?

Criminals posing as Cryptocurrency traders will offer to open a Cryptocurrency wallet with a genuine crypto currency seller in your name, but never give you access.

They may even ask you to provide copies of your identity documents (e.g. passport, driving license) and /or take a selfie to open the cryptocurrency wallet. If you didn't set the wallet up yourself or can't access the money in the wallet, this is a scam. You should stop making payments immediately

Have you checked the cryptocurrency provider is on the FCA register?
Cryptocurrency sellers must register with the FCA. Always use a firm that is registered with the FCA.

Scam Warning !: Paying Tradesperson or for building work.

Could this be a payment redirection scam? .

Criminals often attempt to intercept emails and send you fake account details which appear genuine. Pause, Stop and Think! Please ensure that you check the payment details by phone or in person. This could save you from possible scam.

Scam Warning !: Payment related to Something else.

Could this be scam? Are you feeling rushed into making this payment? Take time to think.

Criminals tricked their victim into sending money directly from their account to an account which they controls. Criminals pose as a genuine individual or organisation and contacting the victim using a range of methods including via the telephone, email and text message and claiming to be from Police, HMRC or their Bank. Criminals also use social media to approach victims.

In all these cases before paying, Pause, Stop and Think! If you decide to proceed and the payment turns out to be a scam, you will lose your money.