Jordan International Bank

Authorised Push Payment (APP) scams

An Authorised Push Payment (APP) scam is when a scammer tricks victims into sending money to someone it's not intended for, by pretending to be someone they know and trust. At times, they will convince victims to send money to someone for what they thought was a genuine purpose, but it was part of a scam.

Payments related to APP scams can be over the phone, online or in person and most are completed instantly. Scammers will try to pressure its victims into deciding, or more importantly making a payment, before they are able to realise that they are a victim of a scam.

Examples of APP scams

Impersonation scams

This is where criminals gain a customer's trust by impersonating trusted individuals or organisations such as banks, family, friends, HMRC, the police, delivery companies, and others to trick them into transferring money. The victim may then authorise a transaction, believing they are making a legitimate payment.

A criminal could also say that your bank account is at risk and ask you to move your money to a safe account. So, if you experience any of the above, you should stop all interactions and report this immediately.

Purchase Scams

Criminals often fake items on social media, websites or marketplaces which don't exist. This usually means you pay for items and services which don't exist. These could be designer clothes, tech gadgets, holidays and tickets. If you're asked to pay straight away and the seller is being pushy this is most likely a scammer.

Remember if something feels too good to be true then it most likely is. Always check the legitimacy of the seller, their reviews to see if they are genuine and if you're asked to transfer directly into an account this should alert you that something isn't right.

Romance Scams

Romance scams occur when fraudsters imitate or develop a fake persona with the intent of getting money from their victims. This is very common online and usually the 'romance' is built on lies to gain sympathy and trust from their victims. At times, they will fabricate stories to make their victims panic for the fraudsters' safety or health resulting in giving away their savings and money to them.

This type of scam is on the increase. If anyone asks for money in these situations, you should be aware it's likely to be a scam. Speak to your family, friends, or us for advice.

Investment Scams

Victims are often taken in by the promise of high returns if they transfer money thinking it's a genuine investment but its most likely fraudulent. The investment could be in anything including property, cryptocurrency, or land. Scammers usually will not provide any documentation or legitimate contracts. As previously stated, if it sounds too good to be true it usually is.

New Rules relating to APP Scams

From 7 October 2024, new rules will be introduced to reimburse victims of APP fraud. The Payment Services Regulator (PSR) has recognised the significant impact that APP scams are having on customers.

Victims of APP fraud can make a claim to their bank which will be then fully investigated and if the criteria is met, the victims will be reimbursed for the amount lost to the APP scam.

The APP fraud reimbursement rules apply to Faster Payments and CHAPS payments. In most cases we will aim to decide on your claim in 5 business days. However, in some cases we may need extra time, and it could take up to 35 business days to resolve this.

What's not covered under the new rules?

- APP scams where the final payment was made more than 13 months before you report it.
- Payments you've made to another account that you have control over.
- International payments.
- You've acted fraudulently yourself – including if you've lied or misrepresented your circumstances for financial gain.
- Civil disputes between you and a person or company you're paying.
- If you don't meet the measures through gross negligence in the Consumer Standard of Caution (please see below).

The Consumer Standard of Caution

Under the new rules, customers are expected to take certain steps before and after making a payment.

- Customers will be expected to provide any information requested as part of the investigation, if customers fail to do this then this could prevent claims for reimbursement being successful.
- report the scam to Action Fraud Police.
- Tell us immediately if you think you've been a victim of a scam.
- Do not ignore any warnings given by us or another organisation which would put you at risk of being a victim of a scam.