Case Study 2025

Unauthorised payments following OTP scam

Fraud

What happened

A couple received a phone call from someone claiming to be their bank warning them about suspicious payments on their joint account.

Believing the call was genuine, they confirmed some of their account details. During the call, a one-time passcode (OTP) was disclosed to the fraudster who then used it to register a new device.

Shortly afterwards, three payments totalling **£4,750** were made from the account without the couple's knowledge or consent.

The bank said that use of the OTP meant the payments ***were authorised*** under its terms and conditions.

What we considered

- the nature of the scam and its impact on the couple
- whether sharing an OTP amounts to authorisation of the transaction
- whether it was fair and reasonable for the bank to rely on its own exclusion of liability where there was customer carelessness
- whether the couple's actions objectively met the threshold of gross negligence
- what the bank did to prevent the customer sharing the OTP inappropriately

What we found

- the couple believed they were dealing with their bank
- the payments were not authorised by the customer
- sharing the OTP may have been careless but did not amount to gross negligence
- the bank's warnings were not sufficient to shift the liability to the couple

COMPLAINT UPHELD – the bank was required to refund the loss and pay compensation for distress & inconvenience

Key learnings

Being deceived into sharing an OTP during a scam does not automatically mean a customer authorises a payment. Each case must be assessed on what is fair and reasonable, taking account of its context including reasonable belief about who they are in communication with, clarity of warnings, and the circumstances at the time.