Case Study 2025

Multiple unauthorised payments following an impersonation scam

Fraud

What happened

Sarah's work colleague received a scam call claiming to be from Sarah's bank and saying a fraud had been detected on her account. The colleague then sent Sarah a note giving her the number the scammer gave for her to call back. Sarah called the number.

During the call, she was persuaded to log into her online banking, install third-party software and share multiple security codes, enabling the fraudster to gain remote access to her devices, resulting in **£24,000** being stolen.

Despite feeling uneasy at points, she continued to follow their instructions.

The bank declined to reimburse her, stating she ignored warnings, shared security codes and allowed remote access to her devices.

What we considered

- the nature of the scam and its impact on Sarah
- whether Sarah's actions objectively met the threshold of gross negligence
- whether the bank acted reasonably in allowing the payments to proceed
- whether the bank acted quickly enough upon notification of the scam to recall the funds from the receiving bank

What we found

- Sarah believed she was dealing with her bank
- multiple security codes and account credentials were disclosed, and the account security was compromised
- the bank provided clear warnings not to share the security codes
- Sarah's actions met the threshold of gross negligence

COMPLAINT NOT UPHELD – the bank was not required to reimburse the loss

Key learnings

Where a customer takes numerous separate actions that compromise account security, and ignores real-time warnings, their conduct can amount to gross negligence. In this case, it's the combined impact of the customer's actions, not just one error, that resulted in the customer being held responsible.