DRN-4298696

The complaint

Mr D complains that Nationwide Building Society ("Nationwide") hasn't refunded the full amount of £14,500 which he lost when he fell victim to an impersonation scam.

What happened

The details of this complaint are well known to both parties and have also been set out previously by the investigator. So, I don't intend to repeat everything again here. I'll only provide an overview and focus on giving my reasons for my decision.

In December 2022, Mr D fell victim to an impersonation scam. He was contacted by an individual claiming to be from an e-commerce company, with whom he already had an account. Mr D was told that several purchases totalling £4,000 had been approved on his e-commerce account.

Mr D followed the caller's instructions and, under the guise of preventing the completion of these purchases, two faster payments – £10,000 and £3,500 – were made from his Nationwide account to another individual's account. A third payment was detected by Nationwide's systems as unusual and was prevented. The caller then asked Mr D to register his card with a money remittance service so that a compensation payment could be made to him. Following this, two card payments were attempted but these were also blocked by Nationwide. Mr D realised he'd been scammed when he didn't receive the promised compensation and the caller asked him to purchase gift cards from his local shop.

Nationwide was able to recover £10 from the beneficiary's account. It also refunded 50% of the remaining loss under the Contingent Reimbursement Model (CRM) Code.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

Having done so, I agree with the conclusions reached by the investigator for the following reasons:

- Mr D submits he didn't realise at the time that he'd made the payments. So the first thing I need to decide is whether, on balance, I think he authorised the disputed payments.

- In line with the Payment Services Regulations 2017 (PSRs), broadly speaking, Mr D is responsible for any payments that he has authorised, and he isn't responsible for unauthorised payments. The PSRs explain that authorisation depends on whether the payment transaction was authenticated correctly and whether the consumer consented to it.

- There doesn't appear to be any dispute over whether the payment transactions were properly authenticated – Mr D's security credentials were used on both occasions

given he's told us he logged on to his Nationwide account and entered the payment details. Thinking about consent next, in the context of PSRs this isn't the same as 'informed' consent. If a customer uses the agreed form and procedure for making a payment order, then they've given consent.

- Nationwide's terms and conditions set out the form and procedure for making payments to another account – providing information about where the payment is going (i.e., account details and the amount). The terms state that Nationwide also checks that the payment request has come from the customer. It does this by asking a combination of log in / security details, biometric information, card reader, security codes, and confirming the payment details. Given Mr D would have needed to complete the agreed steps (i.e., logging on, entering the payee account details as well as the amount, and confirming those details), under the PSRs he'd be considered to have consented to the transactions.

- Mr D says he didn't realise payments were being made at the time – he questioned why he was keying the transaction amounts and the caller told him they were numerical codes to block the payments and not amounts. I acknowledge that he might not have fully understood what was happening at the time and was likely tricked into taking the actions that he did. But that's not a consideration under the PSRs in whether the payments were authorised. As I'm satisfied that the transactions were authenticated correctly and that Mr D consented to them, they're considered authorised. And that means the starting position is that Mr D is liable for the payments.

- There's no dispute that Mr D has been the victim of a scam. Under the provisions of the CRM Code, both the payment service provider and its customer have obligations. If it can be shown that the customer has met their requisite level of care, then they will receive full reimbursement. If the customer has not done this, then it is for the firm to show that it has met its obligations under the Code. If a firm has not met its obligations, then, subject to any liability by the bank which received the money, it will be liable for 50% of the customer's loss.

- Nationwide has already accepted its actions fell below the required standards. I understand that Mr D doesn't recall seeing any warnings at the time of keying in the payment details, but the evidence suggests otherwise. Nevertheless, Nationwide accepts that the warning it provided him wasn't effective in compliance with the Code. But Nationwide also submits that Mr D hasn't met the requisite level of care, which means it is only liable to reimburse him in part. So, I've gone on to consider that next.

- Having carefully considered the circumstances of this case, I don't think Mr D had reasonable basis for believing that the transaction and/or the person he was transacting with was legitimate. I say this because:

    - When questioned about it, he said he didn't check that the number he'd received the call from did in fact belong to the e-commerce company. No attempts were made to verify that the call was genuine.

    - The caller showed Mr D the purported purchases on his e-commerce account after he downloaded the remote access software. But Mr D didn't verify this information independently by logging on to his e-commerce account and checking the status for himself.

    - Mr D has previously made faster payments from his Nationwide account, so it's reasonable that he would have known what the payment process looks like. Yet he completed the same steps and authorised the scam payments, including selecting 'friends and relative' as the payment purpose, despite the caller claiming that the information he was being asked to enter in the payment fields were numerical codes to block the purchases.

- Given neither Nationwide nor Mr D met their obligations under the Code, I find that the 50% reimbursement which Mr D has already received from Nationwide is fair in these circumstances.

- Notwithstanding the reimbursement under the provisions of the Code, if I were to consider whether Nationwide could have prevented the payments from being sent in the first instance, I'm not persuaded that the overall outcome would change. This is because even if I were to make a finding that Nationwide ought to have questioned the payments before releasing them, and that this would likely have stopped Mr D in his tracks, I would then go on to consider whether he is partly to blame for what happened. And whether it would be fair to make a deduction for contributory negligence. Much for the reasons I've given for why I don't think Mr D had a reasonable basis for believing that the payment or the person he was transacting with was legitimate, I'd be concluding that he is equally responsible for what happened and so it would be fair to make a 50% deduction for contributory negligence.

I appreciate that this will come as a disappointment to Mr D, and I'm sorry to hear about the situation he's found himself in. However, I'm not persuaded that Nationwide needs to do anything more here.

My final decision

For the reasons given, my final decision is that I don't uphold this complaint as Nationwide Building Society has already fairly resolved it.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr D to accept or reject my decision before 21 September 2023.

Gagandeep Singh
Ombudsman