

## The complaint

Mr N, helped by a family representative, complained because Nationwide Building Society refused to refund him for payments which he said he didn't make.

## What happened

There were multiple transactions on Mr N's Nationwide account on 5 May 2023. At the start of the day, his balance was £10.36. In order, his statement shows the payments were:

- A new bill payment, set up using Mr N's registered mobile. This was for £1 and the details entered were Description "Friend" and Reference "Owed."
- A bank credit of £6,292.05. Mr N subsequently explained that he'd recently reached his 18<sup>th</sup> birthday, and this money was from a trust fund, which he said he was looking forward to spending.
- A £10 cash withdrawal, then a £950 payment to the same payee with description "Friend", reference "Owed";
- A £250 cash machine withdrawal;
- Five more payments to the payee with description "Friend", reference "Owed", for £950, £945, £948, £949, and £950;
- A £40 cash machine withdrawal;
- A £250 payment to the payee with description "Friend", reference "Owed."

The balance was then £59.41. There were then small payments to retailers the next day, 6 May.

Mr N contacted Nationwide. Nationwide hasn't been able to provide us with a call recording or chat copy for this, nor any evidence about when this initial reporting of the disputed transactions took place. Its notes indicate there was some contact on 5 May, but there's no detail on this. Nationwide also hasn't provided us with notes about what was said when Mr N reported the disputed transactions, or what its fraud team asked Mr N or what he replied.

However, Mr N provided a screen shot of part of a chat. This doesn't give a date, nor does it show that it was with Nationwide. However, this chat asks a number of questions, which may have been a dialogue with Nationwide. Among other things, this chat asked Mr N:

- whether anyone had access to his card, PIN, mobile or security details. Mr N answered no;
- whether he'd lost his mobile or card around the time of the transactions. Mr N answered that he'd lost his previous card but had received a new one in April;
- whether he knew the named recipient of the funds. Mr N replied that he'd never heard of him;

- Mr N said that he had been robbed in 2022 and he'd reported the card stolen at that point, so he thought someone might have had his information from that time;
- The chat asked whether Mr N recognised the small payments to a bakery and a shop on 6 May. Mr N said he'd been in that location at the time but couldn't remember as it had been a long time ago. He said one of the payments might have been him, but the other wasn't. As Mr N said the transactions had been a long time ago, it's unlikely that this was part of any report to Nationwide in May.

On 28 June, Mr N contacted this service. He said he'd been waiting for the trust fund money, which had gone into his account on 5 May then disappeared. He said Nationwide had blocked his account and card, and had asked him to take proof to a local branch that the incoming money was his. This was about the credit on 5 May and also for three incoming payments from another individual on 28 April for £440, £350 and £350. Mr N said he didn't know anything about the April incoming payments. Mr N said he hadn't heard from Nationwide after that. He wanted his money back.

This service contacted Nationwide. Nationwide sent notes of an undated conversation with Mr N, where he said he hadn't written down his PIN, and no-one had access to his mobile or security details. Nationwide asked him if he'd told anyone his PIN, and he said just some family. Mr N said he'd been robbed in 2022, which he had reported to Nationwide at the time, so he thought someone might have had his information from that time.

Nationwide sent Mr N its final response letter on 5 July. This letter said it had told Mr N that the money transferred out had been done using Mr N's online banking and his card. It said that Mr N was welcome to speak to its fraud team, but they'd need to understand how anyone had access to Mr N's card and his internet banking.

Mr N told our investigator that neither he nor his family knew who had withdrawn his money, and he wanted his money back.

Our investigator didn't uphold Mr N's complaint. He said that online banking records showed that the mobile used to make the bank transfers was the device registered to Mr N, and this phone had been used for previous undisputed transfers. The login to set up the transfer recipient had been recorded as being done using Touch ID – which could only have been done by Mr N. And some of the transactions had been made using two factor identification. As Mr N had his card and hadn't shared his security information, it could only have been Mr N who made the transactions.

Mr N, helped by his family representative, disagreed. He said they'd be talking to solicitors, as Mr N wasn't a criminal and he was purely a victim of fraud. He said Nationwide had failed him, and he hadn't transferred the money himself. And he said his phone didn't have his fingerprint, only his face. Mr N asked for an ombudsman's decision.

### **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.

There are regulations which govern disputed transactions. The relevant regulations here are the Payment Services Regulations 2017. In general terms, the bank is liable if the customer didn't authorise the payments, and the customer is liable if they did authorise them. So I've considered whether it's more likely that Mr N, or a third party fraudster, carried out the disputed transactions.

I asked Nationwide for more information. It didn't have all the information I requested, particularly about the chronology of Mr N's complaint to Nationwide, and this is reflected in the events I've set out above. But where evidence is missing, I take my decision on the evidence I do have, to decide what's more likely than not to have happened. And I do have the technical computer evidence, which in this case is persuasive.

For the bank payments out of Mr N's account, the person carrying out the transactions would have needed access to Mr N's registered phone, and his login credentials:

- The computer records show that the disputed transactions were carried out using the same brand and model of phone that Mr N had used for many previous transactions, which he hadn't disputed. Mr N told our investigator that he has a newer phone model. But it doesn't make any difference if he's since changed it – the important point is that the phone used for the disputed transactions matches other undisputed transactions which Mr N had made.
- The internet banking computer records show that no other devices had been added shortly before the disputed transactions.
- The computer records also show that logins were carried out using Touch ID. I recognise that Mr N said he doesn't have fingerprint ID on his phone. However, the same method of login was used for previous, undisputed transactions. So one of the things I asked Nationwide was about this. It replied that its label "Touch ID" for this computer record was generic and included all biometric access, not just fingerprint. Mr N's phone was protected by Face ID, which is a biometric form of identification. So I accept that it was biometric identification, ie Face ID, which was used for the disputed payments, using Mr N's registered phone.
- Some of the disputed bank payments were carried out using two factor authentication. Nationwide confirmed that this meant the person making them would have needed Mr N's genuine card, PIN, and card reader. Mr N said he hadn't shared any security information, and still had his card.

Whoever carried out the transactions would have needed a significant amount of Mr N's information, access to his phone, and biometric access (in Mr N's case, Face ID) to his phone. So I can't see how any third party could have carried out the bank payments.

For the cash machine withdrawals, the person carrying out the transactions would have needed Mr N's genuine card, and his PIN:

- Mr N didn't say he'd lost his card when he reported the disputed transactions. And he did say that he might have made one of the subsequent small transactions the next day. I can't see how any third party could have obtained Mr N's card without his knowledge on 5 May, carried out the three disputed cash withdrawals, then returned it to him the same day without his knowledge.
- Mr N said that no-one else had access to his PIN. There are 10,000 possible combinations of a four digit PIN. So it's most unlikely any third party fraudster could have guessed the correct PIN.

I've also borne in mind that the withdrawals started as soon as Mr N's trust payment arrived in the account. This indicates that whoever carried them out knew that the payment was expected, and exactly when it had arrived.

Mr N suggested that whoever stole his card in 2022 could have had his information from that time. I don't consider that's a plausible explanation for what happened here. First, that card was replaced and the technical evidence shows that it wasn't the one used for the disputed cash withdrawals. Secondly, the theft of a card in 2022 wouldn't have enabled a fraudster to have accessed Mr N's online banking, mobile phone, and Face ID, a year later. And although there wasn't a large amount in Mr N's account until the trust payment arrived on 5 May 2023, a typical fraudster would have attempted to withdraw what they could immediately when the card was stolen in 2022. They wouldn't have waited a year, and nor is any such person likely to have known exactly when Mr N's trust payment would credit his account.

Taking all these factors into account, I consider it's more likely than not that Mr N carried out the disputed transactions himself.

### **My final decision**

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr N to accept or reject my decision before 6 March 2024.

Belinda Knight  
**Ombudsman**