DRN-4250135

The complaint

Miss S complained because National Westminster Bank Plc refused to refund her for payments which she said she didn't authorise.

What happened

On 17 July 2022, Miss S was shopping, and her handbag was stolen while she was trying on some shoes. The handbag contained her purse, NatWest card and her phone.

Miss S rang NatWest's lost and stolen line at 19:11 the same day, from her mother's phone, to report what had happened. She told NatWest that she had reported it to the police and she needed to stop the debit card immediately. The adviser cancelled the debit card and ordered a new one. Miss S asked if there had been any transactions, and the adviser confirmed there had been none. The adviser told Miss S that she could get cash out using her mobile app, and Miss S replied that her mobile had been stolen as well, as it was in the same bag. The adviser replied that she could go to a branch for cash.

At 20:25 on 19 July, a £1,000 faster payment debit was made to a new payee from Miss S's phone. Another £1,000 payment to the same payee went through just after midnight. At 8:48 on 20 July, a £250 payment was made to a new payee. This took Miss S's account into overdraft.

Miss S contacted NatWest about these transactions on 20 July, and said she hadn't authorised them. NatWest's fraud team investigated.

Meanwhile, Miss S gradually discovered that her other financial accounts had also had money taken from them. She updated the online police crime report with these.

NatWest contacted the recipient bank, and retrieved £5 which it credited to Miss S's account on 28 July. But on 2 August it sent its final response letter to Miss S, saying that the evidence suggested that the payments had been made by Miss S, or by someone with her authority. Miss S asked NatWest to review this, but it confirmed its decision.

Miss S wasn't satisfied and contacted this service.

Our investigator didn't uphold Miss S's complaint. She said that the transactions had been made using the mobile banking app, so someone had access to Miss S's phone and app. Miss S had said that her bank cards, driving licence and phone had all been in her handbag when it was stolen, but she'd said she hadn't saved her mobile banking security information on her phone or written it down. So the investigator thought it was highly unlikely someone else could have accessed her mobile app, so it was most likely that Miss S had made the transactions herself. She also said that if a fraudster had made the transactions, they'd have been likely to make them very rapidly, not with spacing between them.

Miss S didn't agree. She said she hadn't orchestrated the transfers, and hadn't authorised anyone else to make them. She asked us to look at the other parts of the fraud, where the same recipient names had appeared in the debits from her other, non-NatWest, accounts.

She said that all except NatWest had agreed it was fraud, and only NatWest, with whom she'd banked for many years, hadn't believed her. Mis S asked for an ombudsman's decision.

My provisional decision

I issued a provisional decision on this complaint. This was because I'd come to a different conclusion to the investigator. Issuing a provisional decision gave both sides the opportunity to comment on it, by the date set, before I issued a final decision

Before issuing the provisional decision, I considered all the available evidence and arguments to decide what would be fair and reasonable in the circumstances of this complaint.

In my provisional decision, I explained that 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. The regulations also say that account holders can still be liable for unauthorised payments under certain circumstances – for example if they've failed to keep their details secure to such an extent that it can be termed *''gross negligence."*

Miss S reported the thefts promptly both to the police and to NatWest, and she provided evidence about numerous other losses. Whoever carried out the transactions, however, would have needed to know Miss S's mobile banking details. Miss S said that she hadn't saved these on her phone, so it's hard to see how a third party fraudster could have carried out the transactions. It's also very unusual for any fraudster not to take out as much money as possible straightaway – and here, the first disputed transaction didn't take place until 19 July. So here are some unusual features here, which doesn't entirely fit the pattern of a normal theft and fraudulent transactions.

But the deciding factor here is that when Miss S reported the theft of her bag, debit card and phone on 17 July, NatWest only stopped her debit card. The disputed transactions were carried out two days later using the mobile banking app on Miss S's phone, which she had told NatWest had been stolen.

I asked NatWest why it hadn't blocked Miss S's account after her 17 July phone call. It replied that it wouldn't have disabled her online banking, but on that call it should have discussed with her how the stolen device could have been removed from her mobile banking app. NatWest pointed out that the thief wouldn't have been able to access her phone and login details, unless they'd been stored in her bag or on her phone. So she couldn't have kept these details secure. So NatWest offered Miss S 50% of her loss, but Miss S didn't accept this.

I considered this carefully. It concerned me that there was no clear way in which the thief could have found out Miss S's security details if she hadn't stored them in her bag or on her phone, which broke the terms and conditions of the account.

However:

- chronologically, the disputed transactions would never have reached that stage if NatWest's phone adviser on 17 July had correctly acted to prevent the stolen device being used for transactions;
- I would also have expected NatWest's security systems to have triggered when the disputed transactions were attempted. They were out of character for Miss S's account; they were to new payees; and they took her into overdraft.

This case is finely balanced, but as NatWest's phone adviser could have prevented the transactions if he'd told Miss S how the stolen phone could have been removed from her mobile banking app, I found that NatWest was liable. So I said in my provisional decision that, subject to responses from the parties, I intended to order NatWest to refund Miss S.

Responses to my provisional decision

NatWest accepted the provisional decision, and agreed to the recommendations in it.

Miss S also accepted the provisional decision. She sent some media links and said that she wanted me to look at these in relation to fraud via stolen mobiles on banking apps.

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 reconsidered all the available evidence and arguments, and having considered the replies from NatWest and Miss S, I find that my original conclusions were fair and reasonable in all the circumstances of this complaint.

My final decision

My final decision is that I order NatWest to pay Mis S £2,245. This is the total of the three disputed transactions less the £5 which NatWest recovered and returned to Miss S.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss S to accept or reject my decision before 14 August 2023.

Belinda Knight
Ombudsman