DRN-4204953

The complaint

Mrs H complains that Nationwide Building Society ("Nationwide") won't refund transactions she didn't make or otherwise authorise.

Mrs H is being represented by a relative, Mr B, in bringing this complaint.

What happened

Mrs H says that on 5 January 2023, Nationwide sent her a text message asking her to call back in relation to recent activity on her account. It was then that she discovered several payments had been made from her current account earlier that day. Before it spoke to Mrs H, Nationwide had already blocked most of the card payments. It had also stopped a faster payment which it had been instructed to execute.

Nationwide asked Mrs H about the payments which had debited, and she said she didn't recognise any of them. She was asked if she'd received any calls that day and whether she had shared her card or log-in details or been asked to download software on her laptop under the guise of fixing any issues she may have been experiencing with it. Mrs H said that she hadn't spoken to anyone that day and hadn't downloaded or been asked to download any software on her laptop. She also told Nationwide that she hadn't shared her security details with a third party.

Mr B reached out to the merchants directly on Mrs H's behalf and some of the payments were refunded, leaving one debit card payment of £498 and five faster payments of £101.99 each still in dispute.

Nationwide investigated the claim and ultimately declined it, saying the payments were completed using Mrs H's security details. For the faster payments, it said that online banking access was gained through a card reader using Mrs H's card and its associated PIN. Mrs H said she hadn't used her card reader that day or shared any codes with someone.

It later transpired that remote access software was found on Mrs H's laptop. A complaint was made when Nationwide didn't respond to this additional information. It apologised for its service failings and sent Mrs H a cheque for £75 in recognition of this. But Nationwide maintained its position regarding the outcome of her claim.

Unhappy with Nationwide's refusal to refund the disputed transactions, the matter was referred to our service. Our investigator concluded that based on what Mrs H had said about what happened and the technical evidence we'd received from Nationwide, they couldn't see a point of compromise that would have allowed the payments to be made by a third party. So, under the relevant regulations – the Payment Services Regulations 2017 (PSRs) – the transaction would be deemed authorised and Mrs H would be liable.

The investigator said they appreciated that there may be more to what happened at the time of these payments. But without knowing, and based on the available evidence, they didn't believe Nationwide needed to refund the payments.

Mr B didn't agree with the investigator's findings. So, the complaint has been passed to me to decide.

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.

Firstly, I'm sorry to hear that this incident has left Mrs H distressed. I'd like to reassure her, Mr B, and Nationwide that although I've only given an overview of what happened, I've read and considered everything we've been provided in its entirety.

When considering what's fair and reasonable, I'm required to take into account relevant law and regulations; the regulator's rules, guidance and standards; the codes of practice; and, where relevant, what I consider good industry practice at the relevant time.

Where there's a dispute about what happened, and the evidence is incomplete or contradictory, I must make my decision on the balance of probabilities – in other words, what I consider most likely to have happened in light of the available evidence.

Generally, Nationwide can hold Mrs H liable for the disputed transactions if the evidence suggests it's more likely than not that she made or authorised the transactions herself.

In this case, it's not in dispute that Mrs H's personalised credentials were used to make the disputed transactions. The technical data Nationwide has provided shows that her card details (card number and CVV code) were used for the debit card payment. For the faster payments, I've seen evidence that Mrs H's card and its associated PIN were used in a card reader to access online banking each time a payment was made. And the card reader was also involved in at least some of the payments (the ones subsequently refunded by the merchant concerned) to undergo additional verification. So, the payment transactions were authenticated correctly.

But the regulations relevant to this case say that authentication isn't, on its own, enough for Nationwide to hold Mrs H liable. I also need to think about whether the evidence suggests that she, or someone acting with her authority, consented to the transactions being made.

To decide whether Mrs H – or someone acting with her authority – made the transactions, I've carefully considered what she's told us about what happened. And I've considered that in conjunction with a review of the available evidence.

Mr B has told us that Mrs H didn't speak to anyone else on the day in question. At the time, he also told Nationwide that he'd looked at Mrs H's call log and her last call had been nearly a week earlier. More recently, Mr B told us that he would describe Mrs H as quite scam aware and very cautious. And so, he doesn't believe that she could have answered unknown calls and used her card reader several times and disclosed the codes to an unknown person. Mr B submits that Mrs H's card was likely cloned and used by a third party. He believes Nationwide should honour its Digital Banking Promise, which says that it will protect its customers and issue refunds if money is taken without their authorisation (with some exceptions).

I acknowledge Mr B's comments and the strength of his feelings on the matter. But I have to consider all the information before me, including the technical evidence which Nationwide has provided. A card reader-generated code was used to log in to Mrs H's account at least ten times on the day of the disputed transaction. And although the data doesn't show that

every single faster payment also went through additional verification requiring a card reader-generated code, I can see that some did.

That means the physical card was inserted into the card reader, and the PIN entered, on multiple occasions to generate a code for logging in to Mrs H's online banking or approving a payment. Card readers are universal, but they read the chip information on the card. To my knowledge, chip information can't be copied over to cloned cards. That means Mrs H's genuine card would have been used to generate the card reader codes to gain access to online banking and approve some of the transactions. During the call with Nationwide, Mrs H said she hadn't shared her security information with anyone. And there's no suggestion that her card wasn't in her possession at the relevant time.

It's also worth noting that although Mrs H has said she didn't log on to her Nationwide account until after it had sent her a text message, the technical data I've seen shows that the account was accessed through an iPad just a few minutes before the first log in using the card reader-generated code. It is my understanding that the iPad belongs to Mrs H which she has used to access her Nationwide account previously.

When the case came to me, I requested further information from Mr B through our investigator particularly about the remote access software that was found installed on Mrs H's laptop and whether he'd spoken to her about how that came to be. He said the only thing they'd been able to attribute any suspicion to was that a few days prior to 5 January, Mrs H had received an email purporting to be from a money transfer service asking her to click on a link to contact them as she owed them money. Mr B explained that Mrs H was cautious and didn't click on the link. She did, however, reply to the email demanding to know how she owed the firm money when she didn't have an account with them.

From what Mr B has told us, it seems likely that Mrs H received and responded to a phishing email. But if she didn't click on any links and share details like her card number etc., or grant permission for someone to access to her device, it seems unlikely that her security details were compromised at that point.

I've given this a lot of thought. As Mrs H says she didn't disclose her card's PIN or her online banking log-in details to anyone else, and as her card was in her possession during that time, I can't see how the transactions could have been made without some form of involvement on Mrs H's part. Given the steps required, and the number of times those steps would have needed to be completed, I find it unlikely that the transactions were completed without her involvement.

Like the investigator said, I think there may be more to what happened that day than what Nationwide and our service have been made aware of. But Mr B has recently told us that there's nothing more Mrs H can recall about that day. He says the first unusual thing that day was the contact from Nationwide.

Overall, I can't say for sure what happened. But I only have to reach a decision based on the balance of probabilities, i.e., what I think is more likely than not to have happened. I've weighed up everything and given the discrepancies and a lack of plausible explanation, I don't consider it fair to tell Nationwide to reimburse the transactions that are still in dispute, including under its Digital Banking Promise.

I recognise that Mrs H and Mr B will likely be extremely disappointed with this outcome. But based on the available evidence, I can't safely conclude that Nationwide has been unreasonable in holding her liable. Because of this, I won't be asking it to do anything further.

My final decision

For the reasons given, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs H to accept or reject my decision before 16 November 2023.

Gagandeep Singh
Ombudsman