DRN-2964324

The complaint

Mr A complains that Nationwide Building Society registered a marker against him at CIFAS, the national fraud database.

What happened

Mr A has said that he lost his debit card and was unaware that a large payment, in excess of £25,000 had been paid into his account. He says he only found out about the payment once his account was closed.

Nationwide have said that Mr A's account received a large payment which was later confirmed as fraud by the sending bank. Account details and online banking records show that the bulk of the funds were transferred or spent within a few days of receiving them.

Nationwide believed that Mr A was responsible for making the transactions and knew about the incoming fraudulent payment. Once Nationwide received confirmation that the funds were a result of fraudulent activity, they returned the remainder back to the sender's account. Nationwide took the decision to close Mr A's account and register a marker against him at CIFAS, the national fraud database.

Mr A complained to Nationwide and denied he was involved in the transaction or the subsequent spending. He told Nationwide that the CIFAs marker was causing him difficulties trying to open another bank account and asked them to remove it. He admitted he'd been negligent but wasn't involved in any fraud.

Nationwide declined to change their position and Mr A brought his complaint to our service for an independent review. It was looked into by one of our investigators who sought additional evidence from Mr A and Nationwide. Mr A explained that he'd lost his wallet with his Nationwide card around the time of the payment and wasn't responsible for the transactions. He also said his online banking details were in his wallet but couldn't be sure if his personal identification number (PIN) was also in it. He confirmed he still had his phone and the PIN was recorded on the notes section of the phone. He said he didn't use the account much, which was why he didn't notice the card was missing.

Mr A also said he didn't check his online account and only realised there was a problem when he realised he was locked out of it. He continued to deny any knowledge of the fraudulent payment or the subsequent payments made from his account.

Nationwide provided further information about the incoming payment, that the payment had been confirmed as fraudulent by the sending bank. Nationwide also supplied an audit of Mr A's online banking usage.

Our investigator thought Mr A was responsible for making the payments from his account and knew about the incoming payments. He thought it was reasonable for Nationwide to register a marker against him with CIFAS.

Mr A continued to disagree and asked for a further review of his complaint which has now been passed to me for a 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.

In order to register this marker, Nationwide needed to have reasonable grounds to believe that Mr A misused his account, which went beyond a suspicion or concern, and which had appropriate supporting evidence. Having carefully considered everything that both sides have said and provided, I currently think there are sufficient grounds to keep this marker in place. I'll explain why.

The crux of this complaint is that Mr A contends he didn't know anything about the incoming fraudulent payment and wasn't responsible for making any payments from his account related to this transfer. So, I've gone on to consider Mr A's version of the events.

Mr A said he didn't access his online banking because the account only received small payments and wasn't used much. I've examined the online banking audit provided by Nationwide which shows that Mr A's account was regularly accessed on the day's leading up to the incoming fraudulent payment. These "logins" used Mr A's mobile phone through the use of "Touch ID" – which means his mobile phone used biometric security to open Nationwide's banking app, together with additional security information.

The audit shows Mr A's phone was being used to check the statements and make online transfers. On the day of the incoming fraudulent payment his account was accessed over a dozen times throughout the day and several outgoing transfers were made. This was repeated the following day and by this time the bulk of the fraudulent payment had been transferred or moved from the account. Access to the online account was blocked later that day by Nationwide. Mr A's phone was never reported lost or stolen and the biometric protection he used to access the banking app means it's unlikely anyone other than Mr A was using the phone around the time of the incoming fraudulent payment and the corresponding transfers out of the account. The repeated use of the account to check the balance and make payments would seem to indicate that Mr A was waiting for the payment to arrive, before transferring it out again to various accounts.

There were other payments made from the account, including a branch visit using Mr A's debit card and Nationwide's records show a withdrawal for £2,000 was made the morning after receiving the incoming fraudulent payment. Later that same morning, Nationwide's records show Mr A visited a different branch – recorded as a "face to face" visit. There's no further detail of the visit but Nationwide were satisfied the person visiting them was Mr A.

It's possible the withdrawal was done by someone else using Mr A's card, but I don't think it's the likely explanation. If an imposter had taken Mr A's wallet and used his card and other details to arrange the takeover of his account, I'm not sure why they would risk going into a branch. There would be a risk of discovery and a likelihood that evidence of their visit would be captured for use by the authorities. I think they would be more likely to minimise their exposure and just transfer funds electronically or use the card to make purchases, rather than personally visiting two different branches.

So, when taking everything into account, I think Mr A likely knew about the incoming payments because of the extensive use of his mobile banking and the online transfers used to send large payments to other accounts. I think he remained in possession of his card and used them to withdraw funds from his account – and Nationwide's records show that it was

Mr A who made the visit(s) after receiving the fraudulent payment.

Because I've made a finding that I think Mr A more than likely knew about the incoming payment and was responsible for transferring the funds or withdrawing them from his account, it follows that he was aware that this was an unusual situation. I don't know if Mr A knew the specific details of where the money came from or the background to the theft, but I find it likely he was aware the funds weren't from a legitimate source. The pattern of transactions closely follows what we'd expect to see from this type of activity and by that I mean the receipt of a payment into an account and then numerous payments and transfers to move on the funds. There's often a payment made to the account holder – and Nationwide's records show £2,000 cash being withdrawn by Mr A.

So, I think Nationwide had more than just suspicions that Mr A was involved with this fraud, rather than his account being taken over without his knowledge. Once Nationwide received confirmation from the sending bank that their account holder had confirmed the payment was fraudulent, I think Nationwide then had reasonable grounds to believe the funds were related to fraud or financial crime.

But that's not enough to register a marker, the evidence Nationwide relied on also had to be more than mere suspicion. Nationwide received confirmation that the funds were fraudulent and then gave Mr A an opportunity to explain what happened. They then compared all this information to draw their conclusions. As a result of their own investigation, they didn't believe Mr A's version of events. As I've already explained, Mr A's version of events isn't supported by the evidence of how his account was used. He denied any knowledge of the funds and their subsequent removal – but his use of the online banking indicates that he was aware of the payment and then took an active part in sending it to other accounts, as well as removing funds in cash. Because of this, I'm satisfied that Nationwide had more than suspicion and could have reported this to the Police if they wished.

Taking everything into account I think Nationwide met the standards for lodging a marker with CIFAS related to how Mr A used his account and I won't be asking them to remove it.

My final decision

My final decision is that I don't uphold this complaint against Nationwide Building Society.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 25 February 2022.

David Perry
Ombudsman