DRN-3326937

The complaint

Mr A complains that National Westminster Bank Plc unfairly lodged a marker against him with CIFAS.

What happened

Mr A's account was closed by NatWest in 2017. He later became aware that a marker had been lodged against him by NatWest with a fraud prevention organisation called CIFAS.

Mr A believed this was linked to the receipt of fraudulent funds into his account which he's said had nothing to do with him. Mr A explained that at the time, he was away from home studying and was living in shared accommodation. He believes that other students gained access to his private banking information and set up payments out of his account and used his debit card without permission.

Mr A was interviewed by the police about the fraudulent funds, but they didn't pursue the matter.

Mr A believes the use of his account was to enable fraudulent funds to be paid into it without his knowledge. At the time the funds were paid into his account, NatWest had already started a review of the account activity and blocked access to it. This meant the funds were prevented from moving and shortly after they were received into the account, NatWest received information from the sending bank that the funds were the result of fraud. They were later returned to the sending bank's customer.

Once Mr A finished his studies, he complained to NatWest about the marker and asked them to remove it because he wasn't involved in the receipt of fraudulent funds and knew nothing about them. NatWest declined to change their position and Mr A brought his complaint to the Financial Ombudsman for an independent review.

Mr A's complaint was looked into by one of our investigators who asked for information and evidence from all the parties. Mr A gave his account about what happened and explained that because the police didn't pursue any action, this was evidence he wasn't involved in the receipt of the fraudulent funds. NatWest provided evidence of the fraudulent funds and other account activity they were concerned about.

Mr A's complaint wasn't upheld, but Mr A was unhappy with how it had been handled. Mr A's complaint was reinvestigated, and further information obtained, including Mr A's recollection of what had happened at the time. Mr A thought that person's unknown had found his details, including his debit card, security number and online banking details which he often left on his desk or in his room where he was staying. Mr A explained that it was possible for others to have gained access to his room and obtained all these details.

The second investigator didn't uphold the complaint, believing it unlikely anyone else had been involved in setting up online payments and identified Mr A was using his online account around the time the fraudulent funds were received. Mr A commented that the police believed it was only his card details that were used by these unidentified persons. He 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.

When NatWest received reports from the sending banks about the fraudulent funds, they believed they had sufficient evidence to lodge a marker with CIFAS. In order to do this, NatWest have to meet strict standards (known as "pillars") laid down by CIFAS. The two most relevant "pillars" to this complaint are:

- That there are reasonable grounds to believe that a Fraud or Financial Crime has been committed or attempted.

- That the evidence must be clear, relevant and rigorous such that the member could confidently report the conduct of the Subject to the police.

NatWest received reports from the sending banks about the two fraudulent payments, which detailed the way the funds had been stolen and diverted to Mr A's account. I'm satisfied that once NatWest received these reports, they met the criteria of the first pillar.

Mr A has explained that he knew nothing about the fraudulent funds and also didn't recognise several small payments sent from his account to a series of new payees. These payees were set up using Mr A's internet banking access. He also disputed a debit card payment made around the same time.

Mr A believed persons unknown to him had obtained all his banking details and his debit card from his room. They used the banking details to log in to his account and set up several new payees. It's Mr A's case that his account was effectively taken over to enable the receipt of the fraudulent funds and because the police didn't pursue any action, this was evidence that he wasn't involved.

Just prior to the receipt of the fraudulent funds into Mr A's account, NatWest were already reviewing the way the account was operating and had decided to close it. This meant that online access was blocked, so when fraudulent funds were received into it, they were unable to be moved.

The crux of this complaint is whether Mr A was involved in any of the arrangements linked to the stolen funds or not. If, as he's explained, his account was used without his knowledge, then it wouldn't be appropriate for NatWest to hold him responsible for the suspicious activity on his account.

Mr A has stated that his details were taken without his knowledge. He described a situation where he left his debit card/Personal Identification Number (PIN) and various online banking security information in his room which was found by unknown persons.

I appreciate Mr A couldn't remember specifically where he'd left these details because it was several years ago. But, for anyone other than Mr A to have set up these online payments, they would have required a lot of very specific information about his account. I think it's somewhat implausible that it was all available in his room for someone to find. I can understand how some information may have been left, for example his debit card – but not all the other information needed to access his account and set up new payees which also required additional security steps.

When I examined the online audit of Mr A's banking, it's apparent that Mr A had a consistent device prior to the "take over" of his account, which was used before any suspicious account activity took place. It was that device that was logging into the account just prior to and just after the four new payees were set up. It seems unlikely that the same device Mr A usually used was also used by these unknown persons. In order to do that, they would need Mr A's specific device, the details to open the device and the security details needed to access his online banking before returning it to him without his knowledge. So, I don't think it was anyone other than Mr A logging into his account with his normal device over this period.

There are other devices linked to the account which appear after the new payees were set up. I don't know if they were Mr A's, but I think it's more likely than not that he was aware of what was happening with his account because he was logging into it at the relevant times. So, even if other "devices" had logged into his account and were carried out by other persons – I think Mr A was more than likely aware of this.

There was a gap of about two weeks between setting up the new payees and receipt of the first fraudulent payment. If an unidentified third party was responsible for setting these up – then it was a relatively long gap to when they received these funds. This meant there was an increasing likelihood that Mr A would notice these new payees. It seems quite a risk to take unless whoever else was involved in the fraudulent activity knew Mr A's account was "safe" to receive these funds.

I think the relevance of these new payees is they were set up to prepare the account for the incoming fraudulent funds. The four new accounts each had £1 sent to them and this would have meant that any further outgoing payments – such as removing the fraudulent funds – would have been treated as "usual" accounts, making them less likely to be subject to any further banking checks. But because NatWest already had concerns about the account, the funds were blocked as soon as they arrived in the account.

Mr A commented that he was told by the police that these persons must have gotten hold of his debit card to enact the fraud. He said he was unaware of the online activity. I can't comment on any police enquiry, but it's apparent that Mr A's account was used to set up new payees – which as I've explained above was, I think, integral to the incoming fraudulent payments.

Mr A also denied making a payment with his debit card around the same time as the new payees were set up. I can't know for sure if it was him who made them, and it's possible that his debit card and PIN were found by unknown persons and used without his knowledge. Although there's no record of any notice made to NatWest about the lost card, so I don't think that Mr A reported it to them.

I don't think this is the likely explanation. It seems implausible that Mr A's card was stolen around the same time suspicious activity was also taking place on his account. I've already made a finding about Mr A's involvement with setting up new payees, so I think it was more likely than not that it was also him or persons with his consent who used the debit card to make the disputed payment.

I understand Mr A's point about the police choosing not to pursue any action – which he's said is evidence he wasn't involved in the fraudulent activity. But, that's not the criteria for lodging a marker with CIFAS. The criteria is that NatWest *could* report it, not that it must be reported. It's not clear who reported the circumstances to the police and for the purposes of this complaint against NatWest, I don't think it's particularly relevant. That's because I'm satisfied NatWest met the second pillar and I won't be upholding this complaint.

My final decision

My final decision is that I do not uphold this complaint against National Westminster Bank Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 30 May 2022.

David Perry
Ombudsman