

The complaint

Mr B has complained that National Westminster Bank Plc (“NatWest”) failed to protect him from falling victim to an employment-based scam.

What happened

The background of this complaint is already known to both parties, so I won’t repeat all of it here. But I’ll summarise the key points and then focus on explaining the reason for my decision.

Mr B explains that in November 2023 he was contacted by an individual (“the scammer”) on a popular messaging app, offering him the opportunity to work remotely. Mr B expressed an interest in the role, and the scammer explained that the job involved clicking electronic adverts online.

Mr B says the scammer opened a training account for him with the work platform he’d be using to complete the tasks, and also helped him to open a cryptocurrency trading account. It doesn’t appear that he received an employment contract.

Mr B explains that occasionally he noticed that the work account fell into a negative balance, and the scammer explained that he was required to deposit funds into his work account in order to clear the negative balance and continue working. Mr B realised he’d been scammed when the amount he was required to pay increased to £2,900, at which point he says he cut contact with the scammer and contacted NatWest.

Mr B made the transactions from his NatWest account to another account he held in his own name held with company R. The majority of the transactions, with the exception of the one for £400, were made as card payments through Apple Pay. The £400 transaction was a bank transfer. When the funds arrived in Mr B’s other account he then purchased cryptocurrency which he sent on to the scammer.

The payments Mr B made were as follows:

Amount	Date
14/11/2023	£20
16/11/2023	£75
16/11/2023	£30
16/11/2023	£30
18/11/2023	£1,300
18/11/2023	£1,400
18/11/2023	£400
Total	£3,255

Mr B made a complaint to NatWest as he said it should’ve had systems in place to detect and prevent scams of this nature. He said that the payments he made were out of character

compared to the transactions he usually makes. NatWest didn't uphold Mr B's complaint as it said it didn't recognise the transactions as particularly high-risk, so it didn't intervene. It also said the funds being sent from NatWest wasn't the point at which Mr B lost them.

Mr B remained unhappy so he referred the complaint to this service.

Our investigator considered everything and didn't think the complaint should be upheld. He explained that he didn't think the payments Mr B had sent were so out of the ordinary that NatWest ought to have identified them and prevented them from being made. He also agreed that the funds hadn't been lost at the point they left NatWest; as they'd been sent to another account in Mr B's control before being sent to the scammer.

As Mr B didn't accept the investigator's opinion, the case has been passed to me to make 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.

I'm sorry to disappoint Mr B but having considered everything I'm afraid I'm not upholding his complaint, broadly for the same reasons as our investigator, which I've set out below.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And in this case it's not in question whether Mr B authorised these payments from leaving his account. It's accepted by all parties that Mr B gave the instructions to NatWest and NatWest made the payments in line with those instructions, and in line with the terms and conditions of Mr B's account.

But that doesn't always mean that the business should follow every instruction without asking further questions or intervening to ensure requests coming from their customers are firstly genuine, and secondly won't result in harm.

Having reviewed the transactions in question, I'm afraid I don't think NatWest should've stopped the payments or done anything else before it followed Mr B's instruction to pay them.

I say this because the transactions started off as very modest amounts, which were in line with Mr B's general account activity. The transactions for £1,300 and £1,400 were still relatively modest, both individually and combined, when considering the wider landscape of the transactions NatWest generally sees. This, plus the fact that the payments were being made to Mr B's own account with a different provider, and were not identifiably being made to purchase cryptocurrency, means I think it's fair that NatWest didn't consider these payments to be particularly high risk nor that it needed to intervene before it allowed them to be made.

Like our investigator, I also agree that NatWest isn't responsible for Mr B's losses as they didn't occur when the funds left his NatWest account. As Mr B appears to have used the receiving account to purchase cryptocurrency, which he then forwarded to the scammer, he'll need to report the scam with his other account provider, and he may also consider contacting the cryptocurrency exchange provider.

Whilst I don't doubt that this has been a very stressful situation for Mr B, in considering whether NatWest did what it should've done to prevent this scam, I've also thought about Mr B's actions.

Although it doesn't appear that Mr B found it unusual that he was contacted out of the blue with the offer of employment, it's very unusual for companies to contact a prospective candidate and offer them a job through a messaging app, without having spoken to them. Mr B also hadn't received any kind of paperwork or employment contract showing what he thought he'd been offered, or what he'd agreed to do in return, by the time he started making payments to the scammers. This, as well as having to pay in cryptocurrency to earn money in return, isn't a plausible scenario, so I don't think Mr B did enough to protect himself from financial harm.

I do note that Mr B has highlighted that his case has all of the hallmarks of a cryptocurrency fraud, and he's provided messages showing how he was convinced to send money to the scammer. I should explain that I fully accept that Mr B was scammed and it's unfortunate that then scammers had such a detailed and sophisticated way of convincing Mr B they were genuine. But I don't agree that NatWest should have known about, or been suspicious of, what happened – especially as the payments in question had no link to the cryptocurrency transactions that they ultimately funded.

Mr B has also likened his case to an example case he found on the Financial Ombudsman Service's website. Whilst there are some similarities, all cases have their own set of facts, and I don't agree that everything in Mr B's case and the example case are the same – so I'm afraid that doesn't change my decision here.

Recovery of the funds

I've considered whether NatWest ought to have attempted to recover the funds Mr B sent as part of the scam.

In relation to the £300 payment, Mr B sent the funds to an account in his own name, that he had control of, and he then purchased cryptocurrency. The account receiving the funds was therefore not a fraudulent account, nor part of the scam, so NatWest couldn't recover anything from it.

In relation to the other payments, as Mr B used Apple Pay to make some of the payments to his other account, I've considered whether the chargeback process would be relevant here.

Whilst the chargeback process is a relevant consideration in this case, the scenarios in which a chargeback can be raised are limited, and they don't include scams. Based on everything I know about these transactions, Mr B used Apple Pay to transfer funds to his own account, and he received those funds and was able to use them.

I'd only expect NatWest to raise a chargeback if it was likely to succeed in recovery of the funds using that route. But in this case, as Mr B paid himself, and not the scammer, he'd effectively be making a chargeback claim against himself. With this in mind there wasn't a reasonable prospect of success, so I don't think it was unfair that NatWest didn't pursue this route.

I'm very sorry that Mr B has fallen victim to this scam and I understand this situation has affected his mental health due to his deteriorating financial situation. I do realise that my decision will be disappointing, but for the reasons I've set out above, I don't hold NatWest responsible for that.

My final decision

I don't uphold Mr B's complaint against National Westminster Bank Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 29 October 2024.

Sam Wade
Ombudsman