DRN-4921285

The complaint

Mrs A has complained about the actions of National Westminster Bank Plc (NatWest) after she was the victim of an authorised push payment (APP) job scam.

What happened

In October 2023, Mrs A signed up to an online job opportunity which involved submitting reviews for hotels. Mrs A signed up to the job platform where she would complete tasks and could see her commission building up. Mrs A was later told that she could increase her commission when she received a 'commercial ad order'. This led to her 'balance' on the job platform showing as a negative sum which Mrs A then needed to clear - by way of a deposit (in cryptocurrency) in order to unlock orders and then earn the commission.

In order to make the deposits on the job platform, Mrs A was required to transfer funds to a legitimate cryptocurrency exchange. From there, she purchased cryptocurrency and then moved those funds to what she thought was the job platform (but unbeknown to her at the time was a scammer).

The deposit amounts required began to increase in size and Mrs A was told that she'd need to add funds each time to complete the orders before earning commission. Mrs A followed the instructions of the scammer until the deposit amounts became too high for her to afford. She then realised that she'd been the victim of a scam.

As part of the scam, on 7 October 2023, Mrs A made a transfer of £3,022 from her NatWest account. She attempted a second payment which was stopped and her account was frozen. Mrs A also made payments as part of this scam before and after the NatWest transaction through two different banks (I will refer to a bank R and bank M). Those transactions are subject to two separate complaints with bank R and bank M.

Our investigator didn't uphold the complaint. Whilst he considered NatWest ought to have done more – he didn't think better intervention would have made a difference.

Mrs A didn't agree so the complaint has 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.

Having done so, while I'm sorry that Mrs A has been the victim of a cruel scam, I agree with the conclusions reached by the investigator broadly for the same reasons:

In deciding what's fair and reasonable, I'm required to take into account relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

Where I can't know for certain what has/would have happened, I need to weigh up the evidence available and make my decision on the balance of probabilities – in other words what I think is more likely than not to have happened in the circumstances.

In broad terms, the starting position in law is that NatWest is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the terms and conditions of the customer's account. It's not disputed that Mrs A made and authorised this payment, although I accept that when she did so, she didn't think her funds were at risk.

Although NatWest (and the investigator) considered Mrs A's complaint under the Lending Standard Board's Contingent Reimbursement Model (CRM) Code. The Code only applies to a transfer of funds executed across faster payments between GBP (British pound sterling) accounts in certain circumstances.

In this case, Mrs A made a faster payment to buy genuine cryptocurrency which was then transferred to the scammer via a cryptocurrency account/wallet. These transactions (purchasing cryptocurrency) of themselves are not a scam but rather genuine transactions for the genuine purchase of cryptocurrency. The scam happened after that; by Mrs A moving her cryptocurrency to the scammer. The sending of cryptocurrency isn't a faster payment between two GBP accounts as required by the CRM Code. In short, this type of payment isn't covered by the CRM Code.

However, even though the payment isn't covered by the (CRM) Code, NatWest has wider obligations outside of the that. There are circumstances where it might be appropriate for NatWest, to take additional steps or make additional checks before processing a payment to help protect its customers from the possibility of financial harm from fraud.

In this case, I need to decide whether NatWest acted fairly and reasonably in its dealings with Mrs A when she authorised the payment from her account or whether it could and should have done more before processing it.

Whilst I accept that NatWest could have done more here (as the investigator suggested), I do need to consider whether better intervention by NatWest would have made a difference. As explained above where I don't know for certain, I make my decision on the balance of probabilities – in other words what I think was more likely (than not) to have happened.

Causation is a critical factor in all scam cases. This may limit or extinguish the bank's liability even if I were to conclude that it could and should have acted on clear triggers of unusual or uncharacteristic activity. NatWest's acts or omissions must be the immediate and effective cause of losses that were reasonably foreseeable at the time of the breach. Where that isn't the case, NatWest might not be liable.

This is not a decision I've made lightly, but I'm not convinced further intervention would have made a difference to Mrs A's decision-making. I say this because:

NatWest did in fact intervene. It stopped the payment and spoke to Mrs A over the phone about the payment before processing it. Mrs A repeated the story the scammer had told her to say and said she was making a long-term investment to cryptocurrency.

Natwest did also ask during the call: *Have you been instructed to lie or rechange the reason for your payment in order to have it authorised by the fraud team?*

And Mrs A confirmed that she hadn't.

This was a one-off payment to cryptocurrency and the pattern often associated with jobs scams (of initial modest value payments increasing significantly) wasn't present on the NatWest account. So, Mrs A's response about the payment purpose seemed plausible. NatWest can only reasonably warn of the scam risk it identifies.

That said I think NatWest could have done more here to warn and highlight some of the key features of cryptocurrency investment scams during the call – but that wasn't what Mrs A was falling victim to here. So, I don't think a better warning about cryptocurrency investment scams from NatWest would have resonated with the circumstances in which Mrs A found herself.

And there is evidence from Mrs A other linked cases, that with further intervention – such as blocking payments and freezing her accounts, Mrs A would (more likely than not) have found another way to make the payment.

For example, before Mrs A made the transaction from her NatWest account (and at the start of the scam) – she initially made three card payments to cryptocurrency from bank R. R also blocked a fourth transaction and provided a warning that it *is highly likely that the transactions you are attempting to make are part of a SCAM. We've recently spoken with another customer who attempted very similar transactions to yours – they confirmed it was a scam*.

I can see from the chat messages with the scammer, Mrs A discussed R's messages and questions and the scammer told her:

You just need to tell them that you're buying cryptocurrency for long term savings.

Try not to tell the bank that you're working part-time because banks are very sensitive about online part-time jobs, so just follow my way of answering the bank

Mrs A then went on to share screen shots of R's questions about the payment purpose with the scammer; asking for help in answering the questions. It's clear from the chat messages Mrs A was coached though the whole process and given answers to each question she was asked. When R did not process the payment, Mrs A went on to transfer the funds from bank M.

Again, M also intervened on a second attempted payment from Mrs A's account. It stopped the payment and froze Mrs A's account and asked her questions about the transactions in and out of her account. The scammer told Mrs A "*if M contacts you, just tell them you're buying cryptocurrencies for long term savings*".

The account with M remained frozen and Mrs A went on to make the payment from NatWest.

So I think it's more likely than not that Mrs A wouldn't have fully disclosed the true purpose for the payment. Mrs A gave a plausible answer (investing in cryptocurrency) given the payment was apparently being made to purchase cryptocurrency. And, even if NatWest had taken further steps and stopped the payment and frozen Mrs A's account (as her other banks did), I think it more likely than not Mrs A would have continued to make the payment elsewhere as this is what she did when bank M wouldn't process the payment.

I'm sorry Mrs A has lost a significant amount of money. But for the reasons I've explained, I don't think NatWest, who had no involvement in the scam itself, can be fairly held liable for her losses.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs A to accept or reject my decision before 27 September 2024.

Kathryn Milne
Ombudsman