

The complaint

Mrs B complains National Westminster Bank Plc (NatWest) won't refund the money she lost to a scam.

What happened

In early 2019, Mrs B says she was contacted by an individual ("L") on social media. He had photographs of himself on his profile and lots of connections. They struck up a conversation and, over time, Mrs B came to believe she was in a relationship with L. Unfortunately, it appears he was actually a scammer.

L told Mrs B he was living abroad and working at an orphanage and/or hospital. From June 2019 to October 2022, he asked her to send him money for various purposes, via various recipients. Mrs B sent around £30,000 to the scam from her NatWest account.

When Mrs B saw a television programme about scammers, and L's photograph was shown, she realised she had been scammed. In April 2023, she complained to NatWest (via a professional representative) that it should have done more to protect her when she made the scam payments. When it didn't agree to refund her, she referred the matter to our service.

Our investigator didn't uphold the complaint. They didn't think the payments looked particularly unusual within Mrs B's general account activity, so didn't think NatWest had cause to realise she was at risk when she made the payments. And given the time between when the payments were made and when the scam was reported, they didn't think NatWest could recover the funds.

Mrs B appealed the investigator's outcome. Her representative said several payments were made in branch, so NatWest should have questioned her. Yet it didn't do so effectively, and made no attempts to stop the transactions being processed.

The case was then passed to me. I found the payments likely fell under the scope of the Lending Standards Board's Contingent Reimbursement Model ('the CRM code'), which NatWest has signed up to. The CRM code requires firms to reimburse customers who have been the victim of APP scams in all but a limited number of circumstances.

I requested further information from both sides in order to consider the relevance of the CRM code to Mrs B's dispute. I have summarised the relevant information I received from both sides:

Information from NatWest

- I asked NatWest if the payment methods etc. meant they fell under the scope of the CRM code – and if so whether it had considered if Mrs B was due a refund. NatWest confirmed it applied, but said it hadn't refunded Mrs B as it thought she ought to have realised L wasn't genuine.

- NatWest also provided information showing it flagged concerns about a £6,000 transfer Mrs B attempted as part of the scam in July 2019. Mrs B said she was paying her husband, who she had been married to for 20 years. When questioned on why the recipient didn't match, she said she couldn't send it directly as he was in the UN and needed funds to be let out.
- NatWest didn't allow the payment and followed up with Mrs B. She admitted she had been speaking to someone online, and she was helping him as his accounts were blocked and he needed to send money to a friend. NatWest told her this was a scam. It provided advice on these types of scams and offered to refer Mrs B for further, external support – which she declined.
- Given this, NatWest said it also didn't think it could have prevented the scam – as it appeared Mrs B had attempted to mislead it, and had continued despite its warnings.

Information from Mrs B (via her representative)

- I asked for records of Mrs B's contact with the scammer. She said she no longer had this. Our service provided guidance on how this could be retrieved. Mrs B said she was unable to do this. I asked her professional representative to support her with retrieving this, and to either provide the records – or evidence that it had attempted to retrieve them but hadn't been able to. This hasn't been provided.
- As there was a reference to Mrs B making scam payments from another account, I asked her for records of those payments along with her recollections of any contact with that bank, at the time of the payments or subsequently, about the scam. Her representative initially said she was unwilling to provide this. It then provided statements, along with records showing it had submitted a complaint to that bank. It hasn't provided anything from Mrs B about her recollections of the bank's contact with her at the time.
- The final response letter from Mrs B's other bank showed it refunded her outstanding loss from the payments made from that account. But it also said that, when Mrs B made some transactions in branch, she hadn't been honest about what she was doing. It also said it had found some payments Mrs B had reported as part of the scam, from November 2017 to November 2018, hadn't been connected to the scam.
- The letter also said Mrs B had reported that she had first made payments as L said he had been injured in an attack at the hospital he was working at (based abroad). He then asked for money to help his son, who he claimed had a health condition, and for various other reasons.
- Mrs B provided a breakdown of what she recalled about what she had thought each payment from the NatWest account was for. In this, she said she thought the first payment – to the same recipient as the payment NatWest flagged – was for medical supplies due to a child at the orphanage the recipient worked at with L becoming sick. When I questioned her on why she then told NatWest she was sending money to that recipient in relation to helping L via a friend at the UN, she said she was led to believe they worked at the UN but volunteered at the orphanage.
- I asked Mrs B (via her representative) why she had said NatWest hadn't blocked any payments, and why she resumed making payments towards the scam (some months later) after it advised her of the scam. She said she went to the police but they said they couldn't do anything for her.

I then issued my provisional decision in July 2024 explaining why I wasn't minded to uphold this complaint. In summary, I concluded the CRM code was a relevant consideration in Mrs B's dispute. But I didn't think NatWest should refund her under the terms of the code (or for any other reason).

I invited both parties to provide any further comments or evidence they wanted me to consider when reaching my final decision. Both sides have responded, but neither has provided any further comments (aside from Mrs B's representative confirming she doesn't agree).

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.

As I haven't received any further comments or evidence in response to my provisional findings, I see no reason to depart from them. And so, for the reasons set out below, I've decided not to uphold this complaint.

In line with the relevant regulations – the Payment Services Regulations 2017 – banks are expected to execute authorised payment instructions without undue delay. The starting position is that Mrs B is liable for payments she authorises, even if she was tricked about their purpose etc.

However, when payments are made as the result of an APP scam, there are some circumstances under which a bank might be expected to hold liability for the fraudulent loss incurred. Such as when a payment meets the conditions of the CRM code and no exceptions apply which mean the bank wouldn't be expected to refund the consumer.

A bank cannot rely on an exception if the consumer is deemed vulnerable as defined by the code. That would apply when: *"it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered."*

Given what I have been told about Mrs B's difficult circumstances at the time of the scam, I have carefully considered whether she should be considered vulnerable under the code. While I don't doubt the role Mrs B's circumstances played in what happened, it doesn't appear to me Mrs B was *unable* to protect herself at the time.

For example – Mrs B appears to have been able to engage with NatWest's scam warning (which I understand dissuaded her from proceeding for some time) and the police. She was also able to recognise and halt the scam after seeing information about L on television.

I've therefore gone on to consider whether it is fair for NatWest to rely on any exceptions under the code. As I understand it is relying on an exception that would apply if Mrs B didn't have a reasonable basis of belief regarding the circumstances of the payments she made. From what I've seen, I agree that has been applied fairly.

I'm conscious all but one of the payments Mrs B is disputing from her NatWest account occurred *after* it told her the scenario was a scam. It appears she took this on board enough to contact the police. Yet when she submitted her case to us, Mrs B didn't mention this until NatWest provided its records of the interaction. She previously said it hadn't tried to stop any of the payments, and that she was only alerted to the scam after seeing L named as a scammer on the television several years later.

I have asked Mrs B what persuaded her the scammer was legitimate, and to continue making payments from NatWest to individuals on his instructions, around nine months later. She says she contacted the police, but they weren't able to take things forward. However, that doesn't make it particularly clear why, how or when she was persuaded to continue.

Mrs B has also mentioned the scammer told her the children in the orphanage would die if she didn't make further payments. It seems clear to me that the scammer was using social engineering tactics to manipulate Mrs B into proceeding. But what is still not clear to me is why Mrs B was convinced by this over her contact with her bank, and the police, about the individual being a scammer.

I'm also conscious of the wider circumstances of this scam. As mentioned, it does appear social engineering techniques were used, and I'm also conscious of the trust the scammer must have built up with Mrs B to convince her they were in a relationship. But that also has to be balanced against the warning from her bank, and the wider context that she continued to be given (seemingly) wide ranging reasons to pay various accounts, none held in L's name, over a significant period of time, based on the instructions of someone she had not met.

Mrs B was convinced to send payments to around ten different recipients from her NatWest account, and to additional recipients from other accounts. And some of the reasons given for what she needed to pay, and who she needed to send the funds to, seem quite suspicious.

As an example – the next payment sent from NatWest to the scam following its intervention was in April 2020. Mrs B says she sent £1,000 as L said he had given his clothes away to poor people so needed to buy some more. And she sent it to a new recipient as that was the account L provided her with. This doesn't suggest he gave any reason why the funds had to go to this person rather than to him directly. I also think the reason for the payment sounded suspicious, particularly coming after the bank's warning.

So, for the payments made following NatWest's intervention in July 2019, I'm not persuaded Mrs B had a reasonable basis of belief. This is more so in the context of not having any contact records with the scammer, meaning I can't see if there were any compelling reasons or tactics used which helped convince her L was legitimate following the bank's warning.

However, one payment was made prior to NatWest's intervention - £2,000 sent in June 2019. I don't think the size of this payment ought to have prompted NatWest to be concerned about fraud, unlike the later £6,000 attempted payment. But I've considered if Mrs B had a reasonable basis of belief about that payment.

On balance, I'm not persuaded she did. There are a few reasons for this. Firstly, I asked Mrs B what this payment was for, she said it was for medical supplies at the orphanage L and the recipient worked for. But when Mrs B tried to send the £6,000 payment to this same recipient, it seems she then thought the person worked for the UN with L, and would pass on the funds to him.

I appreciate Mrs B has since clarified she thought the recipient worked for the UN but also volunteered at the orphanage. However, it does strike me as unclear why the alleged UN link wasn't mentioned when she discussed the recipient at the time. As I haven't been provided with records of the contact from the scammer, and bearing in mind how long ago this all happened, I don't find it particularly clear what Mrs B thought this payment was for.

What does seem clear is the payment was sent for the benefit of, or at least at the behest of, L. Mrs B also told NatWest at the time she thought the funds were being sent abroad. Yet the account wasn't held in L's name, and I haven't been provided with much information to make clear why Mrs B thought the funds had to be sent to accounts held by others (as occurred throughout the scam). The funds were also being sent to an account held with another UK bank, rather than being sent abroad.

Mrs B was also sending funds on the instruction of someone she had spoken to online but hadn't met, and hadn't known for that long. While I appreciate there has been mention of what she could hear in various calls, and photographs etc. she was sent, I haven't been provided with records of these – meaning I don't know when they date from, or how convincing they were.

I'm also conscious Mrs B reported payments to the other bank as being part of the scam which were found not to be relevant. To be clear, I don't by any means think this is due to dishonesty on Mrs B's part. But it does give me cause to question the accuracy of what we have been told about the scam. I'm satisfied about the general premise of the scam. But the specific details of what Mrs B believed and was told at each point in time are less clear. And those details are key to determining NatWest's liability under the CRM code (or otherwise).

Overall, I don't think Mrs B had a reasonable basis of belief for these payments. As I don't think she met her obligations under the code, meaning I don't think she is entitled to a full refund, I've gone on to consider if the bank met their obligations – in case it might be fair to expect it to issue a partial refund. However, on a fair and reasonable basis, I must also consider whether any failings had a material impact on Mrs B's losses.

Looking at the amount and characteristics of the payments, I'm not persuaded it was remiss if NatWest didn't offer any further warnings on most of these. However, some were of a size such that, under the terms of the CRM code, I would normally expect NatWest to have effectively warned Mrs B of the potential scam risk associated with those payments. And I do appreciate the argument raised by her representative that, for those payments made in branch, the Banking Protocol would be a relevant consideration.

However, I'm also mindful that, although NatWest still realised the July 2019 payment was part of a scam, Mrs B appears to have tried to mask *some* details about the payment that made the risk more apparent. Such as by claiming the payment was for her husband, rather than someone she had recently met online.

The records I have seen from the other bank also mention Mrs B wasn't honest to them about why she needed the money. It also appears she may have sought to make payments from that other account sooner than when she made further payments from NatWest. And at the point she did make further payments from NatWest, they were sent to different recipients – so the link with the scam it had uncovered wouldn't have been obvious.

In that context, I don't think it's particularly clear NatWest ought to have known/found out enough about what Mrs B was doing to issue a warning effectively tailored to the scam she fell victim to. In those circumstances, she wouldn't be due a refund under the code – as NatWest can't be held in breach of its duty for not issuing an effective warning if it's not been given a fair opportunity to do so.

Moreover, I'm also not persuaded an effective warning would have prevented Mrs B's losses. That is because I think NatWest had already advised her of the scam – yet L managed to persuade her to send further significant sums. Both by sending funds through another bank, and later by sending further payments from NatWest. I'm not sure what else NatWest ought to have warned her about which would have dissuaded her from proceeding – particularly as I don't have contact records to help demonstrate what persuaded her to continue.

I therefore don't think it would be fair and reasonable to direct NatWest to (partially) refund Mrs B under the terms of the code – or under our wider expectations for how banks should monitor for, and respond to, indicators of a scam risk.

As the scam wasn't reported until around six months after the final scam payments, I also don't think NatWest would have been able to successfully recover any funds from the accounts they were sent to. It's common in scams like this that funds are moved on quickly to avoid the chances of them being recovered.

Overall, while I know this will be disappointing for Mrs B, I'm not persuaded it would be fair for me to direct NatWest to refund the loss she is seeking. That is largely due to a lack of information, or a clear account, of this scam. I don't have enough confidence, from the limited information and recollections provided, that NatWest is at fault for this loss.

My final decision

For the reasons given above, 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 B to accept or reject my decision before 6 September 2024.

Rachel Loughlin
Ombudsman