DRN-4874126

The complaint

Miss S, via a representative, complains that National Westminster Bank Plc ("NatWest") didn't do enough to protect her when she fell victim to a scam.

For ease, I'll refer to Miss S throughout this decision.

What happened

The details of this complaint are well known to both parties, so I won't repeat them again here. Instead, I'll summarise what happened and focus on giving the reasons for my decision.

Between May and July 2023, Miss S told us she lost £5,150 to a scam. She made one card payment to what appears to be a training website and four bank transfers to a digital payment platform. She made these payments believing that she was investing in cryptocurrency. But, Miss S realised she'd been the victim of a scam shortly after it was suggested she took out a loan to keep investing.

Miss S complained to NatWest but it didn't uphold her complaint as it doesn't accept liability for the loss. It tried to recover the funds sent to the digital payment platform but was unsuccessful.

Our investigator considered this complaint, but he didn't uphold it. He said the card payment appeared to have been made to a legitimate training site. And he didn't consider the remaining payments to be particularly unusual or suspicious in appearance, so he wouldn't have expected them to flag.

The investigator noted that the payments weren't covered by the Contingent Reimbursement Model (CRM) code. And he didn't think Miss S's circumstances meant that NatWest should have intervened with these payments.

Miss S disagreed. So, the complaint has been passed to me to decide.

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 recognise this will be extremely disappointing for Miss S, and I'm sorry that she's been the victim of a cruel scam, I'm not upholding this complaint. I'll explain my reasons for this.

Before I do, I wanted to refer to the detailed submissions provided by Miss S. I don't intend to be discourteous by not responding to some of the points raised, or not doing so in the same level of detail. But I've carefully considered all the information provided before reaching my decision – and have addressed what I consider to be pertinent to this complaint.

Miss S has told us that remote software was involved as part of this scam. But, whether

Miss S made the payments herself or allowed the scammer to make them on her behalf, there's been no dispute that she was aware of and intending for these payments to be made, albeit not knowing at the time that the payments were being made to a scammer. So, I'm satisfied, as was our investigator, that the payments were authorised.

In broad terms, the starting position is that NatWest would have been expected to process payments that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case, the 2017 regulations) and the terms and conditions of the customer's account. In the first instance, Miss S would be presumed liable for the payments.

However, I've thought carefully about whether NatWest ought to have had grounds to suspect that Miss S might have been at risk of financial harm from fraud, and whether it should therefore have intervened before processing the payments. But I don't think it should have.

As the investigator has said, the first payment – a card payment – was made to a training website. It's unclear precisely how this was connected to the scam, but I can't see any reason why NatWest should have intervened with this payment, particularly as it was for a relatively low sum.

The four remaining payments were all transfers. These weren't for insignificant amounts and were identifiably linked to cryptocurrency. But the sums involved weren't so high, nor were the characteristics of the payments – such as the frequency – so unusual that I'd have expected NatWest to have intervened. A payment of £1,000 was made in May 2023, two payments of £1,000 were made on the same day in June and one payment of £2,000 was made in July 2023. So, I don't think, on the face of it, that NatWest was wrong to process these payments.

But, I've thought carefully about what Miss S has told us in relation to her personal circumstances, and whether this should have alerted NatWest to her being at an increased risk of fraud. I think there's a balance to be struck between intervening when there are grounds to suspect someone is at risk of financial harm and preventing them reasonable usage of their own account and funds.

I've thought about what NatWest knew and reasonably understood of Miss S's situation, including there being no indication that she'd requested her accounts to be treated differently. And I don't think it would have been fair for NatWest to have made assumptions about the impact of Miss S's health condition on her. Looking at the statements provided, none of the payments put Miss S's account into a negative balance – and payments were being made to accounts in her own name. So, on balance and factoring this in alongside what I've said above, I wouldn't have expected NatWest to have stepped in here.

I also note that there was a call in which Miss S asked to raise 'the limit' on her account to £2,000. Evidence provided suggests this call took place on 21 June – seemingly just after she'd made two payments of £1,000. NatWest talked her through how to do this and explained that the transfer limit is something managed by the customer, up to a £20,000 limit, by accessing their own account. But, in essence, NatWest was simply assisting Miss S with a technical query – and she wasn't making a payment. As above, I wouldn't have expected NatWest to assume there was a need to intervene and therefore I wouldn't have expected it to probe further.

As our investigator has said, the payments aren't covered by the CRM code. I appreciate Miss S's strength of feeling around this. However, the payments were made to her own account. Miss S opened this account and was able to access it through an email from the digital payment platform where she was then able to enter her password and move funds.

She withdrew funds on one occasion. The fact this was under the advice of the scammer – and that she simply did as she was directed to – doesn't change that she was able to access and control the account. So, the payments therefore fall outside of the code.

In summary, while I'm very sorry that Miss S has been the victim of a scam, I don't think it would be fair to hold NatWest liable for her losses.

My final decision

For the reasons given above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss S to accept or reject my decision before 20 December 2024.

Melanie Roberts
Ombudsman