DRN-4844248

The complaint

Mr M complains that NATIONAL WESTMINSTER BANK PUBLIC LIMITED COMPANY (NatWest) won't reimburse the funds he lost when he fell victim to a scam.

Mr M is represented in his complaint by a professional third party, but for ease, I will continue to refer to Mr M throughout this complaint

What happened

Mr M says he received a text message from an individual which appeared to be directed to someone else. Mr M responded and the individual apologised but a conversation via a messaging app continued. Mr M understood that he had formed a friendship with the individual, who I will refer to as "the scammer."

The scammer told Mr M that she was a senior cryptocurrency trader with a company and shared a link to its' website. Mr M thought the website appeared professional. He looked online and found positive reviews, which satisfied him that the company was legitimate. After messaging with the scammer, Mr M decided to invest.

On 31 August 2023, Mr M made a card payment of £81.44 to a cryptocurrency platform which was then used to seemingly credit his trading account. After the investment appeared to perform well, on 28 September 2023, Mr M transferred £4,000 to an account opened up in his own name with firm B.

Mr M says he realised that he had been the victim of a scam once he tried to withdraw money from the investment and was asked to pay various fees and taxes.

Mr M says that NatWest failed in its duty of care to him. He thinks the transactions were out of character, so NatWest should have intervened.

NatWest declined to reimburse any funds to Mr M, saying that he would have received the relevant warnings when making the payments. NatWest said that Mr M authorised the payments, so they would not have triggered additional checks. NatWest said it could not recover the funds and suggested that Mr M contact B about the payment he made of £4,000.

Our investigation so far

Our investigator didn't recommend that Mr M's complaint be upheld. She said the cryptocurrency merchant which Mr M paid, was a legitimate business which didn't appear on any warning list. Given the low value of the payment, she didn't think it should have been automatically flagged by NatWest's systems.

In general, our investigator didn't think the payments were particularly unusual or suspicious. She noted that Mr M kept his account balance relatively low. He had a history of crediting his account with large sums before making payments of a similar value. As Mr M didn't interact with NatWest when he made the payments, our investigator didn't think it missed the opportunity to identify that the payments related to a scam.

Our investigator didn't think that as chargeback for the first payment would have been successful. And as Mr M then made an international transfer to an account held in his own name, NatWest could not have attempted recovery. She thought that even if the funds had credited an account which Mr M didn't control, by the time he reported the scam, the funds would have already been moved.

Mr M disagrees with the investigation outcome. He says NatWest should have intervened when he made a high value, international payment to a new account which he'd not used before.

As the complaint has not been resolved informally, it 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.

I appreciate that I have summarised this complaint in less detail than the parties and that I have done so using my own words. The rules that govern us, together with the informal nature of our service, allow me to take this approach. But this doesn't mean I have not read and considered everything the parties have given to us.

Card payments and payments made to an account held in your own name and/or international payments, aren't covered by the CRM Code. So, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make in accordance with the Payment Services Regulations 2017 and the terms and conditions of the customer's account. And I have taken this into account when deciding what is fair and reasonable in this complaint.

But that's not the end of the story. Taking into account the law, regulators' rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider NatWest should fairly and reasonably:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;

- have had systems in place to look out for unusual transactions or other signs that might indicate that its' customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer;

- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect 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 Mr M when he made the payment requests, or whether it should have done more than it did. I have considered the position carefully.

Although Mr M made the first payment to an identifiable cryptocurrency merchant, the value was very low – just over £81. I can't see why this would have appeared suspicious or unusual to NatWest. So, I don't think there was any reason for it to have intervened at the time.

The next disputed transaction was for significantly more - £4,000. However, this was not made to a cryptocurrency merchant. Instead, Mr M made the payment to an account he had set up in his own name with B. Although it was an international payment, I don't consider there were any obvious scam risk factors. There wasn't a history of recent escalating cryptocurrency payments which might have signalled the possibility that Mr M was falling victim to a multi-stage fraud. I also note from Mr M's bank statements that he frequently made payments to a digital remittance service which allows customers to send money online to other countries. And in April 2023 he had credited his NatWest account with over £7,600 before making payments of £2,000 and £5,000 to accounts in his own name. So, in the context of Mr M's account and NatWest's responsibilities, I don't consider it needed to stop the £4,000 transaction as it was not suspicious. Especially as Mr M's account was not left drained as he had already transferred a large amount of money to his current account.

When a payment is made by card, the only recovery option NatWest has is to request a chargeback. As the cryptocurrency merchant provided the service Mr M requested, a chargeback claim would not have been successful. As Mr M made the second payment to an account in his own name and onwards from there, I agree with our investigator that there was no prospect of NatWest being able to recover any of the money. Particularly as Mr M made the payment in September 2023 but didn't raise his concerns about the transaction until December 2023.

Overall, I am not satisfied that NatWest should fairly have intervened in either payment. So, while I am sorry to hear about this cruel scam and Mr M's loss, I don't ask NatWest to reimburse him. And there aren't any ways in which it can recover the funds for him.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 22 April 2025.

Gemma Bowen
Ombudsman