DRN-4922355

The complaint

Miss O complains that NATIONAL WESTMINSTER BANK PUBLIC LIMITED COMPANY ("NatWest") have failed to refund money that Miss O lost as part of a scam.

What happened

Miss O met someone on a social media site who was actually a scammer that I will call B. B said that they invested in a crypto trading company (that was also a scam). On the advice of B, Miss O sent over £65,000 by card payments and bank transfers to a crypto exchange. The funds were then sent to the scam company. These transactions occurred in April and May 2021.

Miss O was unable to withdraw the profits she saw on the scam company website and at this point she realised that she had been scammed.

She raised a complaint with NatWest as she thought that it should have prevented her from sending the funds to the scammer and she requested that she be refunded the transactions in question.

One of our investigators looked into this matter and they did not uphold this complaint.

Miss O did not agree with this and therefore her complaint was passed to me to issue a final 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.

In broad terms, the starting position at law is that a bank such as NatWest is expected to process payments and withdrawals 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.

But, taking into account relevant law, regulators' rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable that NatWest should:

• 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 firms 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, or provided additional warnings, before processing a payment – (as in practice NatWest sometimes does including in relation to card payments);

• have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multistage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

NatWest intervened later in the scam and asked Miss O to attend a branch in order to release a payment. In the scam chat the scammer tells Miss O what to say. It is unclear what was asked in the branch or what Miss O said. But given that the payment was released, I find it unlikely that Miss O was forthcoming with what she was doing. Also, in the scam chat, Miss O makes it clear that she was unhappy with payments being blocked and that as the money was hers, she should be able to do what she wanted with it. It is clear at this point that Miss O completely trusted the scammer and they had formed a close relationship.

Miss O's account was relatively new, so NatWest did not have a long payment history to compare the scam payments too. That said, I think that NatWest should have intervened earlier than it did - specifically when Miss O made a £5,000 payment on 25 April 2021, as this represented over £12,000 sent to a crypto exchange in 7 days.

But even if I think that NatWest should've intervened earlier, I then need to consider if Miss O would have given accurate answers to questions asked about payments earlier on in her relationship with B. I have carefully considered this and based on the scam chats, I think that Miss O and the scammer had already formed a close relationship by the time of the payment in question and Miss O had already seen on the scam platform that she had made a good return on her first few transactions. So had an earlier payment been stopped and questions asked, I think Miss O would have (with the help of the scammer) likely provided answers to any questions posed in a way to ensure that the payments were released. I am also mindful that multi stage scams involving crypto were not as well known in 2021.

So overall I think that NatWest should have intervened earlier than it did. But I do not think that this would have likely stopped or uncovered the scam.

I've also thought about whether NatWest did enough to attempt to recover the money Miss O lost. In this instance, the CRM does not apply t as the payments were to an account in Miss O's own name. I also don't think that a chargeback should have been attempted, as the payments were essentially a means to send funds from her NatWest account to the crypto exchanges - which is what happened.

I appreciate this will come as a disappointment to Miss O, and I'm sorry to hear she has been the victim of a scam. However, I'm not persuaded that NatWest can fairly or reasonably be held liable for her loss in these circumstances.

My final decision

For the reasons given above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss O to accept or reject my decision before 16 July 2025.

Charlie Newton

Ombudsman