Financial Ombudsman Service

The complaint

Mrs C complains that National Westminster Bank Plc (NatWest) is refusing to refund her the amount she lost as the result of a scam.

Mrs C is being represented by a third party. To keep things simple, I will refer to Mrs C throughout my decision.

What happened

The background of this complaint is well known to all parties, so I won't repeat what happened in detail.

In summary, Mrs C was interested in investing with cryptocurrency and had previously made investments in this area. Mrs C found an advertisement on Facebook for a business called MainBit (X) that appeared to be endorsed by well-known celebrities and allowed small initial investments.

Mrs C clicked on the link and started to make a small investment. X explained the investment to Mrs C and helped teach her how to place trades via the screen sharing application AnyDesk.

The investment appeared to be doing well. Mrs C was able to make a small withdrawal and later received a £500 Amazon voucher. Happy with the return Mrs C made further payments into the investment and even took out a loan to fund further investments with X.

Mrs C made the following payments into the investment via a cryptocurrency exchange using her debit card:

Date	Payee	Payment Method	Amount
12 September 2022	CEX.IO	Debit Card	£1,421.18
12 September 2022	CEX.IO	Debit Card	£1,116.64
29 September 2022	CEX.IO	Debit Card	£2,740.84
29 September 2022	CEX.IO	Debit Card	£6,395.29
27October 2022	CEX.IO	Debit Card	£406.06
27 October 2022	CEX.IO	Debit Card	£1,116.64
27 October 2022	CEX.IO	Debit Card	£2,233.28

Mrs C attempted to make a withdrawal from the investment but unfortunately this was not successful, and it became apparent that Mrs C had fallen victim to a scam.

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.

It has not been disputed that Mrs C has fallen victim to a cruel scam. The evidence provided

by both Mrs C and NatWest sets out what happened. What is in dispute is whether NatWest should refund the money Mrs C lost due to the scam.

Recovering the payments Mrs C made

Mrs C made payments into the scam via her debit card. When payments are made by card the only recovery option NatWest has is to request a chargeback.

The chargeback scheme is a voluntary scheme set up to resolve card payment disputes between merchants and cardholders. The card scheme operator ultimately helps settle disputes that can't be resolved between the merchant and the cardholder.

Such arbitration is subject to the rules of the scheme, meaning there are only limited grounds and limited forms of evidence that will be accepted for a chargeback to be considered valid, and potentially succeed. Time limits also apply.

Mrs C was dealing with X, which was the business that instigated the scam. But Mrs C didn't make the debit card payments to the scammer directly, she paid a separate cryptocurrency exchange (CEX.IO). This is important because NatWest was only able to process chargeback claims against the merchant she paid (CEX.IO), not another party.

The service provided by CEX.IO would have been to convert or facilitate conversion of Mrs C's payments into cryptocurrency. Therefore, CEX.IO provided the service that was requested; that being the purchase of the cryptocurrency.

The fact that the cryptocurrency was later transferred elsewhere – to the scammer – doesn't give rise to a valid chargeback claim against the merchant Mrs C paid. As CEX.IO provided the requested service to Mrs C any chargeback attempt would likely fail.

Should NatWest have reasonably prevented the payments Mrs C made?

It has been accepted that Mrs C authorised the payments that were made from her account with NatWest, albeit on X's instruction. So, the starting point here is that Mrs C is responsible.

However, banks and other Payment Services Providers (PSPs) do have a duty to protect against the risk of financial loss due to fraud and/or to undertake due diligence on large transactions to guard against money laundering.

The question here is whether NatWest should have been aware of the scam and stepped in and questioned Mrs C about the payments she was making. And if it had questioned Mrs C, would it have been able to prevent the scam taking place.

Mrs C has told us that she opened a new account with NatWest as her usual account with another bank would not allow her to make payments related to crypto. So, the NatWest account Mrs C used to make the payments into the scam had very little history for NatWest to compare with and say that the payments she was making were unusual compared to her normal spending habits.

The first three payments Mrs C made into the scam were made to a genuine merchant and weren't of such a high value that I would have expected human intervention from NatWest. However, NatWest did send Mrs C a message to confirm the payment being made was genuine which she confirmed.

The largest payment Mrs C made into the scam was for £6,395.29 on 29 September 2022. While this was for a larger value than the previous payments, Mrs C had previously confirmed she was happy making payments to this merchant (CEX.IO) and she had made previous payments to this merchant more than two weeks earlier without complaint. She was therefore starting to develop a pattern of usual spending on her account. So, I don't think it was unreasonable that this larger payment didn't trigger NatWest's fraud prevention systems and that NatWest didn't step into question Mrs C.

The remaining payments Mrs C made were of lower values and the payments were made over a two-month period.

Overall, I don't think the payments Mrs C made were unusual enough for me to suggest that NatWest acted unreasonably by allowing them to go through without having a meaningful conversation with her.

My final decision

I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs C to accept or reject my decision before 5 February 2024.

Terry Woodham
Ombudsman