DRN-4546606

The complaint

Mr E complains that National Westminster Bank Plc (NatWest) is refusing to refund him the amount he lost as the result of a scam.

Mr E is being represented by a third party. To keep things simple, I will refer to Mr E 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, Mr E has told us that he found an online article that appeared to include an interview with a well-known celebrity stating that his main source of income was from crypto investment.

Interested in the opportunity Mr E clicked on the link provided and completed a short questionnaire. Mr E was then contacted by the scam company I will call "X" stating that one of its consultants would be in touch.

X then called Mr E and explained that he had been assigned a dedicated account manager. Mr E was provided with a login to X's trading platform and X explained how the investment would work. Mr E then made an initial payment into the investment.

Mr E was happy with the initial investment as he could see it was generally growing each day.

Mr E was then contacted again by X and offered an investment in Bitcoin. X said it had acquired two Bitcoins and could offer them to Mr E at a significant discount. Mr E agreed to purchase the coins that were added to his account with X. Mr E received what appeared to be an official document confirming the purchase.

Mr E was then upgraded by X to a higher-level account with a more senior person. X explained that it had inside information that a well-known business was going to release their own token and that Mr E could pre-buy the token, promising a profit of 50% when the tokens were released. The investment would cost a total of £250,000. Mr E agreed and made a series of payments before receiving an official document confirming the purchase.

After making all the payments Mr E's account was showing a balance with X of over £1,700,000.00 but X explained that Mr E would have to make payments in relation to withdrawal fees before any withdrawals could be made. Mr E was sent a release authorisation form detailing the amount due which totalled more than £40,000.

Mr E says that although he was promised he would then be able to withdraw the full amount from his account following the fees being paid X suggested trying a smaller amount first.

A withdrawal of £2,000 was attempted and was successful. But when a larger withdrawal of

£20,000 was attempted, it appeared to fail, and Mr E was told by X he would have to make a further payment.

Mr E then carried out further research and discovered he was likely being scammed. He confronted X who denied the scam but said he could no longer be Mr E's account manager.

Throughout the scam Mr E was guided through the investment process using remote access software and was told to open various accounts to facilitate transfers into the investment, some of which were closed, and new accounts had to be opened with other account providers to facilitate transfers.

The following payments were made from Mr E's account with NatWest in relation to the scam:

Payment	Date	Payee	Payment Method	Amount
1	19 June 2023	eToro	Transfer	£3,500
2	19 June 2023	eToro	Transfer	£850
3	20 June 2023	eToro	Transfer	£9,950
4	20 June 2023	eToro	Transfer	£10,000
5	20 June 2023	eToro	Debit Card	£200
6	29 June 2023	eToro	Transfer	£18,500
7	30 June 2023	eToro	Transfer	£18,000
8	3 July 2023	eToro	Transfer	£20,000
9	4 July 2023	eToro	Transfer	£20,000
10	10 July 2023	eToro	Transfer	£10,000
11	10 July 2023	eToro	Transfer	£10,000
12	11 July 2023	eToro	Transfer	£5,000
13	11 July 2023	eToro	Transfer	£13,000
14	12 July 2023	eToro	Transfer	£10,000
15	12 July 2023	eToro	Transfer	£10,000
16	13 July 2023	eToro	Transfer	£10,000
17	13 July 2023	eToro	Transfer	£10,000
18	17 July 2023	eToro	Transfer	£15,000
19	19 July 2023	eToro	Transfer	£6,250

Our Investigator considered Mr E's complaint and didn't think it should be upheld. Mr E disagreed, so this 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.

It has not been disputed that Mr E has fallen victim to a cruel scam. The evidence provided by both Mr E and NatWest sets out what happened. What is in dispute is whether NatWest should refund the money Mr E lost due to the scam.

Recovering the payments Mr E made

Mr E made a payment in relation to the scam from his NatWest account via his debit card and the remaining payments by transfer. 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.

Mr E was dealing with X, which was the business that instigated the scam. But Mr E didn't make the debit card payment to X directly, he paid a separate business that converted the payment into cryptocurrency. This is important because NatWest would only have been able to process chargeback claims against the merchant he paid, not another party (such as X).

The service provided by the business Mr E paid would have been to convert or facilitate conversion of Mr E's payments into cryptocurrency. Therefore, it 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 Mr E paid.

When payments are made by transfer NatWest has limited options available to it to seek recovery. NatWest could ask the operator of the receiving account to refund any funds that remain in the payee's account. But Mr E has told us he made these payments to an account in his name and those funds were then sent as part of the scam. So, if any funds did remain, they would remain within Mr E's control.

With the above in mind, I don't think NatWest had any reasonable options available to it to recover the payments Mr E made.

Should NatWest have reasonably prevented the payments Mr E made?

It has been accepted that Mr E authorised the payments that were made from his NatWest account, albeit on X's instruction. So, the starting point here is that Mr E 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 intervened when the payments were being made. And if it had intervened, would it have been able to prevent the scam taking place.

When Mr E attempted to make payment 3 NatWest did intervene and a telephone conversation took place.

During the call Mr E confirmed the payment was being made to another account in his name that he had held for some time, and that the purpose of the payment would be to use the funds while travelling in another country. Mr E also confirmed that no one had asked him to lie to the bank if questioned about the payments.

The information Mr E provided was not entirely honest. He had not had the account he was transferring the funds to for some time and the payment was in relation to the investment he was making not to use while travelling.

Another intervention took place when Mr E attempted to make a payment in relation to the scam from another account he held elsewhere, and an online chat took place. During this

chat Mr E confirmed he was not being pressured to make payments, he had not been promised unrealistic returns, he had not been contacted by anyone to invest, he was not buying cryptocurrency and he had remote access software downloaded but this was for work purposes.

The above was not entirely true. Mr E had been promised unrealistic returns, he had been contacted after filling in an online form, he was buying cryptocurrency, and although he may have already had the remote access software downloaded I think he should have volunteered the information that he was also using it alongside the investment he was making considering he had been asked if he had download it in relation to the payment he was making.

Mr E has said that NatWest should have done more to uncover the scam and that he answered some of the questions honestly. But I think it's clear that overall, Mr E was willing to give dishonest information to have the payments processed. I think it's unlikely Mr E would have been any more honest had NatWest intervened further.

As giving incorrect information when attempting to make payments would have made it extremely difficult for NatWest to uncover the scam, I don't think it missed an opportunity to prevent the payments Mr E made and it is not responsible for Mr E's loss.

My final decision

I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr E to accept or reject my decision before 3 January 2025.

Terry Woodham
Ombudsman