DRN-5167395

The complaint

X complains that National Westminster Bank Public Limited Company (NatWest) didn't do enough to protect him from the financial harm caused by an investment scam.

X has been represented by a claims management company throughout his complaint. I have referred to them as X's representatives.

What happened

X met and started talking to someone through a dating platform. The conversations carried on in WhatsApp. The person talking to X, suggested he invest in cryptocurrency. The premise being that if X transferred his money to a cryptocurrency exchange and then moved the cryptocurrency to a further platform, they could make them money.

The person X was in conversation with turned out to be a scammer. He saw on a screen showed to him by the scammer, that his cryptocurrency investment had apparently increased to £22,000 but when he tried to make a withdrawal, the scammer told him that he would need to wait until the end of the month. When he tried to withdraw at that stage, after making 8 payments to the scam, he wasn't able to gain access to his account and wasn't able to contact the scammer either.

X through his representatives, said he had transferred and lost £5991.40 spread across 8 payments between 2 April 2024 and 28 May 2024. These payments, ranging from £50 up to £1000 a time, were all paid for by X's NatWest debit card and sent to an account in his name with a cryptocurrency exchange. X's representatives complained to NatWest about this and said it should have done more to stop these payments from being transferred in the first place.

NatWest said the funds were sent directly from X's account held with it, directly to another account held in his name, which was in his control. It said as such no loss occurred as a result of NatWest following X's instructions. It said the payments did not trigger a response from its systems and there wasn't anything that it felt ought to have alerted it to do more than it did. NatWest didn't uphold X's complaint, so because of this, X's representatives complained on his behalf, to our service.

The investigator didn't think NatWest needed to take any action on this occasion and concluded it couldn't have reasonably been expected to protect X against the fraud here. He made that conclusion because he felt the payments were not particularly unusual or suspicious in appearance at that time. He said the amounts were not unusual, in comparison with X's account history, and the payments were well spread across two months. He concluded that there was nothing that NatWest ought to have done here and so he didn't uphold X's complaint.

X's representatives said by 2024 when these payments took place, NatWest should have recognised the payments were to cryptocurrency and carried out checks as they had a higher risk of being associated with fraud. They said the payments in this case did deviate from the customer's usual pattern of spending.

The parties are not in agreement, so X's complaint has been referred to me for a 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.

The parties are not in dispute that the payments in question are to an account with a cryptocurrency provider, in X's name, and in his control. So, as this is the case, I don't think the principles of the Contingent Reimbursement Model (CRM) code apply here. I've therefore not considered this any further.

I'm satisfied X authorised the relevant payments. NatWest would generally be expected to process payments a customer authorises it to make. And under The Payment Services Regulations and the terms and conditions of the account, X is presumed liable for the loss in the first instance, in circumstances where he authorised the payments. However, this isn't the end of the story. Good industry practice was that NatWest ought to have been on the look-out for transactions that were unusual or uncharacteristic to the extent that they might indicate a fraud risk. On spotting such a payment instruction, I would expect NatWest to intervene in a manner proportionate to the risk identified.

In the context of this scam, X transferred funds from his NatWest account to a cryptocurrency exchange account also in his name. Once he had transferred money into his account, this was converted into cryptocurrency and then was sent onto the scammers wallet.

NatWest would have been aware that X was sending payments to a cryptocurrency exchange, and I take X's representative's point that by 2024, it would have been well aware of the associated risks of multiple payments being made from one of its customer's accounts to a cryptocurrency exchange.

However, just because X authorised payments to a cryptocurrency trading account in his own name, this doesn't automatically mean that NatWest ought to have intervened and asked further questions or restricted these payments. Rather, there is a balance to be struck here, and NatWest needed to consider what was going on and whether there was any indication in X's accounts or an unusual pattern which meant it needed to take further action. I have looked at what happened and also considered X's circumstances and his account history.

Having reviewed X's account and the payments he made to the scam, I'm not persuaded NatWest ought to have found any of the payments suspicious, such that it should have intervened. All of the payments were to an account held in X's name, and although this was a new account, I don't think this alone would be considered of a suspicious nature, particularly when there were apparently no other concerning factors about them. I accept that the payments were to a crypto provider, but that doesn't mean payments should automatically be treated as suspicious.

I have looked at the previous payment history of the account X used to make the payments and can see that the amounts in question would not have seemed unusual or out of place. X made a number of similarly sized payments on a regular basis. So, I don't think it would have caused any alarm or concerns when he made payments of upwards of £1000. There was also a gap in time between some of the payments and all of them were spread out over around 2 months. I could not see that there was a concerning acceleration for example in the amount of the payments or the frequency of these transactions. This would have given

NatWest some assurance about the validity of the receiving account, that there were no issues spanning over the two months that X authorised these payments. I can't see looking through them, that there was a point where NatWest ought to have intervened.

So, with what I have concluded in mind, I don't think in the circumstances of X's complaint, that I can fairly say NatWest ought to have done anymore with regards to these payments, for all the reasons I have given.

Finally, I've thought about whether NatWest could have done more to recover the funds after X reported the fraud. This is something in certain circumstances it would have been able to look at once it had been notified about the scam from X. X made the payments through his debit card, and there was potential to recover them through the chargeback scheme.

However, X didn't make the payments to the scammer, instead he made them initially, to a legitimate cryptocurrency exchange. So, NatWest were only able to make chargeback claims against the cryptocurrency exchange, which wouldn't have in any likelihood succeeded given, it had provided its services as described. So, there isn't anything further to consider in this regard.

I'm sorry X was scammed and lost this money, but in conclusion I can't fairly tell NatWest to reimburse him in circumstances where I'm not persuaded it reasonably ought to have prevented the payments or recovered them.

My final decision

My final decision is that I don't uphold X's complaint, and I don't require National Westminster Bank Public Limited Company to do anything further.

Under the rules of the Financial Ombudsman Service, I'm required to ask X to accept or reject my decision before 10 July 2025.

Mark Richardson
Ombudsman