DRN-3983105

The complaint

Mr G complains that National Westminster Bank Plc won't refund the money he lost when he fell victim to a scam.

What happened

Mr G responded to an online advert for a company which claimed to provide cryptocurrency trading advice. On their advice, Mr G moved funds from his NatWest account into cryptocurrency wallets he set up, and he then transferred these on to a supposed trading platform. But when he was ordered to pay an additional fee to withdraw some of his funds from that platform, he realised it was a scam.

Initially, Mr G disputed the matter with NatWest. He then referred his complaint about NatWest to our service. He said it should refund him in line with the Lending Standards Board's Contingent Reimbursement Model (CRM) code, of which NatWest is a signatory. He also said the payments were uncharacteristic, so it should have performed further checks – and if it had, that would have prevented his loss.

Our investigator didn't uphold the complaint. She explained the CRM code didn't apply to these payments. She also didn't think the payments looked unusual enough to warrant further checks from NatWest. But even if they had been flagged, she wasn't convinced NatWest would have uncovered the scam as Mr G had been coached by the scammer on what to say about the payments. She also didn't think it missed an opportunity to recover the lost funds.

Mr G has appealed, so the case has been passed to me to decide. In summary, he says it's common for this type of scam to involve payments to a legitimate cryptocurrency platform. He also argues his payment of just over £10,000 was significantly out of character.

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.

Having done so, I've decided not to uphold it. I'll explain why.

Mr G has confirmed he authorised these payments. In line with the Payment Services Regulations 2017, NatWest is expected to execute authorised payment instructions without undue delay. So the starting position is that Mr G is liable for the payments.

While NatWest is a signatory of the CRM code, under which banks are generally expected to refund victims of authorised push payment scams, it doesn't apply to these payments. That's because they were sent by card, and international transfer, to wallets in Mr G's own name (and under his control). The CRM code doesn't apply to payments made to an account held by the sender. Nor does it cover card payments or international transfers.

However, there are also some situations where we believe that banks—taking into account relevant rules, codes and best practice—ought to have identified a fraud risk, so should have looked at the wider circumstances surrounding the transaction before making the payment.

NatWest hasn't been able to confirm whether any payments were flagged due to the passage of time. So I have considered whether they should have been. And if so, whether appropriate intervention would have prevented Mr G's loss.

The payment destinations wouldn't have been cause for concern – as the payments went to genuine cryptocurrency merchants rather than to a known scammer. But there are other reasons why a bank might identify a payment as presenting a fraud risk. Such as if it is significantly out of character with the customer's usual account activity. And while the payment destination alone wasn't a concern, nor was it a complete reassurance. As Mr G has pointed out, it is common for cryptocurrency scams to involve payments to genuine cryptocurrency merchants to start.

I agree with our investigator that there is a reasonable case for arguing these payments weren't so unusual that NatWest ought to have had concerns. As she highlighted, Mr G had a history of making payments to trading platforms unconnected to the scam. Which made the scam payments appear more expected and in keeping with how the account was normally used.

There were also other high value payments made from the account, which will again have affected the level of spending NatWest would have seen as within normal parameters. And most of the scam payments were in the region of a few hundred points, which didn't look particularly suspicious within Mr G's general spending. I don't think the payment for around £5,000 looked particularly concerning either, given there were other similar value payments made around that time.

I do appreciate the £10,000 did arguably appear to be an escalation. However, even if NatWest had intervened at this point, I agree with our investigator it's unlikely it would have succeeded in stopping the scam. That is because Mr G has told us he was coached by the scammer on what to say if the payments were blocked. This is backed up by the records he has provided of his contact with the scammer. There is, in fact, mention of contact with NatWest around this time – although it's unclear if that was in response to payments being flagged. In response, the scammer told Mr G to say he was just investing by himself, and to not mention third parties.

And so, if NatWest questioned Mr G about the scam payments, it appears likely he would have claimed to be trading by himself without third party involvement. In those circumstances, it seems unlikely to NatWest would have had cause to think something untoward was going on – as the scenario as described wouldn't have matched the usual features of a cryptocurrency scam.

I appreciate Mr G was coached. But the indication is that he didn't answer, or wouldn't have answered, NatWest's questions honestly. And that would have made it more difficult for NatWest to have identified, and protected him from, the scam risk.

In the circumstances, I'm not persuaded any failings by NatWest in processing the payments give fair cause to hold it liable for Mr G's subsequent loss.

I also don't think NatWest missed an opportunity to recover Mr G's fraudulent loss. As set out above, the funds were transferred to Mr G's own wallets with legitimate cryptocurrency companies, before being passed on to the scammer. So NatWest couldn't recall the funds, as they had been moved on. Nor were there probable grounds for successful chargeback claims against the wallet providers, as they provided the expected service by loading the funds to the wallets in line with the payment requests received.

I appreciate this will be disappointing for Mr G, who clearly fell victim to a cruel and sophisticated scam. But I've decided not to direct NatWest to refund him for his loss, or to otherwise compensate him or take further action in relation to his complaint. Overall, I'm not persuaded it should fairly be held at fault for the loss Mr G incurred at the hands of the scammers.

My final decision

For the reasons given above, my final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr G to accept or reject my decision before 23 November 2023.

Rachel Loughlin
Ombudsman