DRN-4716726

The complaint

Mr A complains that National Westminster Bank Plc (NatWest) have failed to refund £1,162 he says he lost to a crypto investment scam.

The details of this complaint are well known to both parties. So, if there's a submission I've not addressed; it isn't because I've ignored the point. It's simply because my findings focus on what I consider to be the central issues in this complaint – that being whether NatWest was responsible for Mr A's loss.

I should also point out that whilst being mindful of previous decisions made by the Financial Ombudsman, I review each case on its own merits.

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 agree with the conclusions reached by our Investigator for the following reasons:

- It isn't in dispute that Mr A authorised the disputed payments he made to a legitimate crypto exchange (which I'll refer to here as 'K') via a genuine payment processing company (which I'll refer to here as 'P'). Mr A has said the funds were then transferred on to the scammers. The payments were as follows:

Date	Payment
17/11/23	£10
17/11/23	£1
20/11/23	£1
20/11/23	£300
21/22/23	£850
Total loss	**£1,162**

- The payments were requested by Mr A using his legitimate security credentials provided by NatWest. In line with the Payment Services Regulations 2017, consumers are liable for payments they authorise. NatWest is expected to process authorised payment instructions without undue delay.
- The Contingent Reimbursement Model (CRM Code) is a voluntary scheme that provides increased protection for victims of authorised push payment scams. NatWest is a signatory of the CRM Code.

- But the CRM Code doesn't apply in the circumstances on Mr A's complaint. While Mr A says he lost money to scammers, his payments went to an account in his own name for the legitimate purchase of crypto, which is not covered under the CRM Code.
- While the CRM Code doesn't apply, I've considered whether NatWest should've done more to prevent Mr A from falling victim to the scam, as there are some situations in which a bank should reasonably have had a closer look at the circumstances surrounding a particular transaction. For example, if it was particularly unusual or suspicious.
- At the time these payments were made there was a high prevalence of crypto scams; and so, the risks of making crypto related payments should've been well known to NatWest. But I must keep in mind that banks process high volumes of transactions each day; and that there is a balance for NatWest to find between allowing customers to be able to use their account and questioning transactions to confirm they're legitimate.
- These payments were also made by way of Open Banking which can make it harder for banks to identify that payments are being made for the purposes of crypto.
- I appreciate that Mr A has lost £1,162 which is a significant amount of money. But this amount wasn't paid in one large transaction. It was spread over five separate smaller increments which, in my judgement, wouldn't have appeared particularly suspicious to NatWest. I'll explain why.
- From looking at Mr A's bank statements in the six months prior to the scam, I can see that the account is generally used for low value day-to-day spending; but there are five payments between April and October 2023 ranging from £347.93 to £443.02. And so, I don't think the first four disputed payments would've appeared particularly out of character.
- I accept that the £850 payment was larger than most previous payments made from Mr A's account. But it isn't unusual for customers to make a larger, one-off payment from their account from time to time, during normal account activity.
- And by the time of this larger payment, 'P' was an existing payee with no concerns having been expressed by Mr A about the payments previously made to 'P'. This, I believe, would've made the £850 payment appear in line with Mr A's previous account activity.
- All payments were also made to an account in Mr A's own name with a legitimate company ('K') via a genuine payment processor ('P'). And I'm also mindful that payments involving the purchase of crypto can be part of a legitimate investment.
- The payments to 'P' were relatively spread out, having been made over a period of five days. This isn't usually conducive with the hallmarks of a scam and would, in my opinion, again have made the payments appear to NatWest more like normal account activity.
- So, having considered the payments Mr A made to 'P', I'm not persuaded, on balance, there was anything unusual or suspicious at the time that ought reasonably to have triggered NatWest's fraud monitoring systems, or that would've indicated he was in the process of being scammed.
- I also agree with our Investigator that there was no reasonable prospect of NatWest recovering the lost funds at the point it was alerted to the scam.

I appreciate this will likely come as a disappointment to Mr A, and I'm sorry to hear of the situation he has found himself in. However, in the circumstances of this complaint, I don't consider it would be fair and reasonable to hold NatWest responsible for Mr A's loss.

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 Mr A to accept or reject my decision **before 17 December 2024.**

Anna Jackson
Ombudsman