DRN-4814771

## The complaint

Mr P complains that National Westminster Bank Plc won't refund money he lost when he was a victim of an investment scam.

Mr P is represented by a firm I'll refer to as 'C'.

## What happened

The background to this complaint is well known to both parties and so I'll only refer to some key events here.

In June 2023, Mr P was researching investment opportunities and came across an advert on a social media platform for a firm I'll refer to as 'CBT' - which turned out to be scam investment firm. Mr P completed their enquiry form, which led to him receiving a call from CBT. Impressed with their professionalism and the investment opportunities presented to him, Mr P decided to invest with CBT.

As part of investing with CBT, Mr P has explained he was required to provide identification and was given a username and password for his trading account – in which he could see trades available to him and investment graphs. He made the following payments as part of the scam:

| Date | Transaction type | Amount |
|---|---|---|
| 30 March 2023 | International transfer | £500 |
| 14 April 2023 | International transfer | £1,600 |
| 12 June 2023 | Faster payment | £2,450 |
| 13 June 2023 | Faster payment | £2,450 |
| 23 June 2023 | Faster payment | £2,082 |
| | **Total** | £9,082 |

The first two payments were sent internationally to the investment scam. The next three payments were sent to an account in Mr P's own name with an Electronic Money Institution (EMI), with the funds forwarded to the scam from there. He says these three payments were made to pay a variety of commission, withdrawal and recovery fees. But despite paying these, Mr P says CBT told him further fees needed to be paid, and he realised he'd been scammed when they refused to release his money.

C complained, on Mr P's behalf, to NatWest on 12 December 2023 saying the payments were made as part of a scam. In short, they said:

- NatWest ought to have robustly questioned Mr P about the purpose of the payments – such as whether he'd thoroughly researched the company or looked online for reviews. This would've allowed Mr P to find negative reviews about CBT and, at this point, he'd have realised he was being scammed.

- In the months prior to the scam, Mr P hadn't processed payments of such high value and hadn't invested in crypto. Yet NatWest failed to intervene and allowed these payments to be debited from Mr P's account.

- NatWest didn't provide investment scam advice effective enough to break the spell of the scammer. Had they done so, the spell of the scam would've been broken, and Mr P wouldn't have lost his funds.

- NatWest failed to protect Mr P from the scam despite these payments being high value and out of character. No specific warnings were provided, as the warnings presented were generic and appear before most legitimate payments he makes.

- To settle this complaint, Mr P would accept a full reimbursement of his losses, 8% interest and £300 compensation.

NatWest didn't uphold the complaint. In short, they said:

- Mr P reported the scam to them in July 2023 and a case was raised for the first two international payments. The beneficiary bank was contacted to see if any funds remained but, unfortunately, it had all been removed.

- Mr P could've carried out more due diligence to ensure it was a genuine investment before making these payments.

- The other three payments were credited to an account in Mr P's own name and so they were unable to accept liability or reimburse this loss as NatWest wasn't the point the loss occurred.

- Their fraud prevention system is set up to monitor activity for the latest fraud trends and if a transaction matches a known trend, a security check will be generated. If, however, a transaction doesn't trigger additional checks which are later reported as fraud, this is not a bank error.

- These payments were made by Mr P using their online banking facility.

- They place appropriate and relevant scam warning messages across their online banking to warn customers of the types of scams they're seeing. And before making a payment a tailored scam warning is displayed, and their customer must confirm they're confident they have read and understood their advice and they're satisfied they have taken relevant steps. Should customers follow their advice, they're confident they wouldn't fall victim to a scam.

- The payments aren't covered under the Contingent Reimbursement Model (CRM) code.

Mr P's complaint was referred to the Financial Ombudsman. Our Investigator didn't however think NatWest had to do anything further. In short, she said:

- She didn't think the first two payments would've been unusual or suspicious in appearance to NatWest based on their value. Nor did she think the £2,450 payment

on 12 June 2023 would've flagged either, as it was similar to Mr P's prior account usage. NatWest did however block this payment before processing it.

- NatWest's records show they contacted Mr P and he confirmed this payment was genuine.

- A Confirmation of Payee (CoP) warning, saying the payee's account couldn't be checked, was provided to Mr P. NatWest also provided online warnings that would've been shown to Mr P at the time of making the payments based on the purpose reason he selected. She thought these were appropriate and highlighted the relevant risks of going ahead with the transaction(s).

- NatWest carried out reasonable and proportionate checks and additional steps before processing the payments based on the risk presented. So, she didn't think NatWest were responsible for Mr P's loss.

- She thought NatWest took reasonable steps to recover Mr P's loss. This included contacting the international beneficiary bank, but they confirmed no funds remained. And the last three payments were sent to an account in Mr P's own name, and so she wouldn't have expected NatWest to have attempted recovery on these.

C disagreed and asked for Mr P's complaint to be reviewed by an Ombudsman. The matter has therefore been passed to me to decide. C added that they believe the amount Mr P was sending – namely the payments on 12 and 13 June 2023 – should've been concerning to NatWest. These payments totalled £4,900 to a new payee, albeit in Mr P's own name. So, further security measures should've been placed on Mr P's account. And they don't believe a CoP warning and written warning was sufficient here given Mr P was transferring funds for crypto purposes.

**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.

I'm sorry Mr P has been the victim of a scam as I appreciate it has impacted him greatly. But while I'm sympathetic to Mr P's circumstances, I must consider whether NatWest is responsible for the loss he has suffered. I know this won't be the outcome Mr P is hoping for but, for similar reasons as our Investigator, I don't think they are. I therefore don't think NatWest has acted unfairly by not refunding the payments. I'll explain why.

I've thought about the CRM code which can offer a potential means of obtaining a refund following scams like this one. But these payments aren't covered by it. This is because the CRM code doesn't cover international payments or payments made to an account held in a person's own name – which is what happened here. I've therefore considered whether NatWest should reimburse Mr P under any of their other obligations.

In broad terms, the starting position in law is that a bank is expected to process payments that their customer authorises them to make. It isn't disputed that Mr P knowingly made the payments from his account – albeit under the direction of the scammer – and so, I'm satisfied he authorised them. Therefore, under the Payment Services Regulations 2017 and the terms of his account, NatWest are expected to process Mr P's payments and he is presumed liable for the loss in the first instance.

However, taking into account the regulatory rules and guidance, relevant codes of practice and good industry practice, there are circumstances where it might be appropriate for

NatWest to take additional steps or make additional checks before processing a payment to help protect customers from the possibility of financial harm from fraud.

So, the starting point here is whether the instructions given by Mr P to NatWest (either individually or collectively) were unusual enough to have expected additional checks to be carried out before the payments were processed. When considering this, I've kept 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.

Having looked at Mr P's prior account usage, his account was typically used for low value day to day transactions. But while I accept some of these payments were of a higher value than Mr P commonly made on his account, it isn't unusual for customers to make larger payments from time to time as part of normal account activity. And I don't think the payments here, either individually or collectively, were of a monetary value whereby I would've expected NatWest to have considered them suspicious or extortionately high. Nor were the payments made in rapid succession or did they deplete Mr P's account balance, which can be indicators of potential fraud. And given the funds were being sent to an account in Mr P's own name with a legitimate EMI, I wouldn't have expected NatWest to have had sufficient reason to suspect Mr P was at risk of financial harm from fraud.

I am however aware that NatWest did, as a security measure, put a block on the £2,450 payment made on 12 June 2023. This was because they wanted to check the payment was genuine before processing it – with NatWest's records suggesting this confirmation was obtained from Mr P via text message. In the circumstances, I think this was a reasonable check to carry out before processing the payment – and that it was proportionate to the identifiable risk at the time (which, as I've said, I don't think there was reason for significant concern.).

I also understand that Mr P was provided with scam warnings as part of the online banking transfer process – with the warnings tailored based on the payment purpose he provided. Considering the above, I think these warnings were similarly reasonable and proportionate to the identifiable risk here. And so, while I note C believes NatWest ought to have undertaken further security measures, I think NatWest took proportionate steps to protect Mr P from financial harm in these circumstances. Unfortunately, there are situations whereby a consumer will lose out, through no fault of their own, but have no recourse to a refund (as the bank likewise aren't at fault).

I've considered whether, on being alerted to the scam, NatWest could reasonably have done anything more to recover Mr P's losses, but I don't think they could. This is because NatWest contacted the international beneficiary bank about the first two payments, but no funds remained. And the funds from the other three payments had already been moved from the account in Mr P's own name. So, any attempt in this respect would've similarly been unsuccessful – but even if funds had remained, Mr P could've accessed these himself and quicker than any recovery attempt by NatWest.

I have a great deal of sympathy for Mr P and the loss he's suffered, as I appreciate it is a significant sum of money to him. But it would only be fair for me to direct NatWest to refund his loss if I thought they were responsible – and I'm not persuaded that this was the case. For the above reasons, I think NatWest has acted fairly and so I'm not going to tell them to do anything further.

**My final decision**

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 P to accept or reject my decision before 26 November 2024.

Daniel O'Dell
**Ombudsman**