

## The complaint

Ms M complains that National Westminster Bank Plc (NatWest) won't refund money she lost when she was the victim of a scam.

Ms M is represented by a firm that 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 January 2021 Ms M was the victim of a crypto scam. She found the scam firm – which I'll refer to as 'W' – on the internet after searching for investment opportunities and found their website professional. Ms M's research also found W as one of the first recommended and so, she didn't doubt their legitimacy. After expressing an interest with W, she was persuaded to invest by them and they convinced her to download remote desktop software. Ms M made the following payments to W via a legitimate crypto exchange:

Date	Type	Amount
19 January 2021	Faster payment	£1,000
20 January 2021	Faster payment	£1,000
21 January 2021	Faster payment	£1,000
22 January 2021	Faster payment	£1,000
Total:		£4,000

Ms M saw she'd made a substantial profit of about £7,000 on the trading platform and wanted to make a withdrawal. W told Ms M she would need to pay fees to do so and, after she said she couldn't afford to, she was encouraged to take out a loan. Ms M refused and told W she wouldn't be able to invest anything more. At this point, W stopped communicating with her and Ms M realised she'd been scammed.

C complained to NatWest, on Ms M's behalf, in March 2023 and – in summary – said:

- Ms M had a reasonable basis to believe the scam was genuine.
- NatWest failed to identify these transactions as unusual for Ms M, as she used the account for general everyday purposes such as shopping and general household bills. And she'd made no transactions of a similar value in the months leading up to the scam.
- NatWest should've spoken with Ms M before processing the transactions and, had this happened, it would've become apparent – through appropriate questioning – that she was falling victim to a scam. From this, the scam payments wouldn't have been made.
- NatWest failed to protect Ms M from the scam by not making such enquiries or providing an effective warning(s).

- To settle the complaint, they said Ms M would accept reimbursement of the monies she lost plus interest and compensation.

NatWest didn't uphold the complaint and explained the payments weren't covered under the Contingent Reimbursement Model (CRM) code. 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 carried out. If a transaction doesn't trigger, this doesn't however mean there's been a bank error. Due to the time since the payments were made, they couldn't say whether any of them did flag for a security check. But looking at Ms M's account, the payments weren't unusual and they could see she made larger transactions after the scam payments. They're also required to make payments in accordance with customer instructions which they did here.

Our Investigator considered the complaint but he didn't think NatWest had to do anything further. He didn't think the payments would've been particularly unusual or suspicious in appearance to NatWest. And he referred to Ms M making a genuine £3,000 transaction on 20 January 2021, prior to the second scam payment. He felt this would've given NatWest less reason to have considered the last three scam payments as suspicious (as they were of a much lesser value). And he added the scam payments didn't deplete Ms M's account or push it into its overdraft. So, he didn't think NatWest should've intervened before releasing the payments. He also added that, given the funds were sent to an account held in Ms M's own name, he wouldn't have expected NatWest to have attempted to recover them.

C disagreed and so the matter has been passed to me to decide. In short, they said:

- The Investigator's conclusions rest on Ms M repaying a portion of funds to her foster child, an account that credited their client with £4,000 the day prior to this payment. Ms M's foster child is also an established payee on the account and cannot be used as a fair comparison as to what NatWest should be expected to flag. There is a clear difference in risk between the legitimate established payee and the new scam payee linked to crypto/trading.
- Ms M made multiple transfers to the crypto exchange over a short period of time. NatWest's systems are designed to pick up on various payment characteristics and, just because Ms M made a payment to an established payee on her account, the beneficiary risk of the scam payee cannot be ignored.

### **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 Ms M has lost a significant sum of money. But while I know this isn't the outcome she's hoping for, I don't think NatWest has acted unfairly by not refunding her loss for similar reasons to our Investigator. I'll explain why.

I've thought about the CRM code which can offer a potential means of obtaining a refund following Authorised Push Payment (APP) scams. But the CRM code only applies to payments made to an account held by another person. As the payments Ms M made were sent to an account she held in her own name with a crypto exchange, they're not covered under the CRM code. I've therefore considered whether NatWest should reimburse Ms M under any of their other obligations.

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

However, taking into account 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 Ms M to NatWest were unusual enough - in relation to her typical account activity - to have expected NatWest to have identified Ms M was at risk of financial harm from fraud.

Having reviewed Ms M's account statements, it was typically used for low value day to day spending along with relatively frequent transactions of several hundred pounds. The four £1,000 payments were therefore for more than Ms M normally spent on her account - except for the £3,000 transfer our Investigator has referred to. That said, banks must strike a balance between allowing customers to be able to use their account and questioning transactions to confirm they're legitimate. And so, I don't think payments of £1,000 would've been unusual enough, in value alone, to have given NatWest sufficient reason to have seen them as suspicious.

I've also considered the frequency of the payments and that the funds were being sent to a new payee for crypto trading purposes. While I accept C's point that multiple payments made to a new payee, over a short period of time, can pose a greater risk than those made to an existing beneficiary, I don't think it necessarily means - in these particular circumstances - that NatWest is responsible for the loss Ms M suffered. This is because the payments were made to a legitimate crypto exchange. And although, sadly, scammers do target individuals looking to grow their savings, many people do invest of their own accord and by genuine means. So, while NatWest should be looking out for signs that their customers are at risk of financial harm from fraud, I'm not persuaded the value or frequency of the payments were so unusual or suspicious for NatWest to have suspected Ms M was at risk of financial harm - thereby prompting them to intervene before processing them.

Taking all of this into consideration, I don't think NatWest ought to have done more before following the instructions Ms M gave.

I'm sorry to hear Ms M suffered a financial loss as a result of what happened. But it would only be fair for me to direct NatWest to refund her loss if I thought the bank was 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 Ms M to accept or reject my decision before 29 September 2023.

Daniel O'Dell  
**Ombudsman**

