DRN-4310249

## The complaint

Miss T complains that National Westminster Bank Plc (NatWest) wouldn't refund money she lost in an investment scam.

## What happened

*What Miss T says:*

Miss T is represented by a third-party firm of solicitors, and I will refer to Miss T as the complainant.

In June 2020, Miss T was out of work due to the pandemic. She started to investigate investment into cryptocurrency as a way of making money. A friend had successfully invested into crypto before. Miss T made some online inquires and was contacted by someone purporting to be from an investment company - which I will call A. This turned out to be a scammer.

The person spent eight weeks talking to Miss T and she came to trust the scammer. Miss T says she went onto review websites at the time and found positive reviews.

Initially, Miss T made a payment of £2 to her account with a payment service provider (which I will call B – which was a well-known payments firm for bitcoin transactions). The scammer helped Miss T set up her account with B, and showed her how to make a payment from B to A. She could then see the payment of £2 appeared in her bitcoin account with the scammer investment company (A).

Within four days, Miss T was told the investment of £2 was already increasing in value and she was told bitcoin was rising in value again. A made a payment of £40.15 to Miss T's account on 10 August 2020 – to show she was making money. The scammer (A) said that an investment of £14,000 would grow by £7,000 in a short period of time. She made a payment of £7,180 on 11 August 2020. This was then shown to grow in value to £11,000 over the next week or so. Miss T was encouraged by this and made a further payment of £7,100 on 19 August 2020. The payments were:

| Date | Method/Beneficiary | Amount |
|---|---|---|
| 6 August 2020 | Faster payments/ Payment service provider B | £2.00 |
| 10 August 2020 | Credit from A | (£40.15) |
| 11 August 2020 | Faster payments/ Payment service provider B | £7,178 |
| 19 August 2020 | Faster payments/ Payment service provider B | £7,100 |
| 24 August 2020 | Credit from A | (£5) |

| | | |
|---|---|---|
| **Total** | | **£14,235** |

Miss T intended to then withdraw the money but the next day, she saw all the money in her trading account with A had disappeared. She then realised she had been scammed. She was contacted again by other people purporting to be from A and was asked to pay fees to get her money back, but she didn't do that.

Miss T says she was ashamed about what happened and is still struggling to come to terms with it. She lost most of her savings – and as she had no work at the time, struggled to keep afloat. She has been stressed and worried about conducting any business online. She says that to this day, she is still playing 'catch up' to recover from the loss of money she suffered.

Miss T argues that NatWest should've done more to protect her. She wasn't given any warnings about the payments. If NatWest had intervened and provided a warning on how to spot investment scams, she says she wouldn't have made the payments. She says NatWest should refund the money paid.

Miss T contacted NatWest in August 2022 – and said NatWest said they couldn't help her. She said the bank were dismissive of her case.

*What NatWest says:*

NatWest said they'd made the payments in accordance with Miss T's instructions and weren't liable. They'd provided online warnings on their website to warn customers of the types of scams being seen.

NatWest said that after March 2018, a message was displayed on the payments screen when a customer made a payment – to warn of the types of scams being seen. These are shown when a payment is being made, or a new payee is being set up. Customers must confirm they're confident with the payment before making each transaction. If a payment matches a known trend, then a security check is carried out.

NatWest said the payments were to Miss T's own account with B. This meant:

- NatWest couldn't be held responsible for Miss T's losses as she then moved the funds from her account with B to the scammer. The point of loss was when Miss T transferred the money from B to A.

- The Contingent Reimbursement Model Code (CRM Code) didn't apply.

- no funds could be recovered – as the funds reached Miss T's account with B before being withdrawn and paid to A.

NatWest apologised for the experience she had when she contacted them about the scam.

*Our investigation so far:*

Miss T brought her complaint to us. Our investigator said the second and third payments were unusual and NatWest should've intervened and asked questions of Miss T. But she was persuaded that even if they had, it was likely that Miss T would've gone ahead and made the payments. This was because:

- She had not been approached ‘out of the blue’ by someone pressurising her to invest, but she had made the inquiry herself.

- She had been looking to invest in cryptocurrency and had a friend who had done so successfully.

- She had done a lot of research online and found nothing suspicious about company A. She said reviews were positive.

- She only made an initial investment of £2, and then discussions took place over several weeks – there wasn’t any pressure for her to send money for a long time.

- She received a credit of £40.15 on 10 August 2020 – so all looked to be genuine.

- NatWest provided an online warning at the point of the payments. Miss T selected *“investing in cryptocurrency (e.g. Bitcoin)”* and then a tailored warning was then presented to her.

**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 to hear that Miss T has lost money in a cruel scam. It’s not in question that she authorised and consented to the payments in this case. So although Miss T didn’t intend for the money to go to a scammer, she is presumed to be liable for the loss in the first instance.

So, in broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer’s account. And I have taken that into account when deciding what is fair and reasonable in this case.
But that is not the end of the story. Taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider NatWest should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) doesn’t apply in this case. That is because it applies to faster payments made to another UK beneficiary – and in this case, the payments were made to Miss T’s own account with B.

I need to decide whether NatWest acted fairly and reasonably in its dealings with Miss T when she made the payments, or whether it should have done more than it did. I have considered the position carefully.

The important matter here is whether these were payments that NatWest might reasonably have considered unusual, and therefore whether they should've held or stopped them and contacted Miss T about them.

I looked at Miss T's account. I think the two larger payments can be considered sufficiently unusual in amount for NatWest to have flagged them and asked questions of Miss T. There were some other payments, but they were of much lower value than the scam payments.

E.g.:

- June 2020: £3,660 – point of sale payment
- June 2020: £1,600 – online payment
- June 2020: £1,000 – BACS payment
- May 2020: £1,585, £2,460, £1,500, £5,000 – online payments
- April 2020: £1,775 – BACS payment
- April 2020: £2,470 – online payment
- March 2020: £1,139 – online payment

The payments in dispute were to a new payee and were for larger amounts than was usual for Miss T to make. And – the payments were to a payment service provider (B) - which was known to make bitcoin payments. So on balance, I'm satisfied that it's reasonable to have expected NatWest to step in, stop the payments and contact Miss T about them. But they didn't.

But – I noted that NatWest told us they presented Miss T with a warning message when she made the payments in question. This said: "*Protect your money from fraud and scams – are you confident that the payment you're about to make isn't a scam? Tell us your payment reason so we can help you protect yourself"…*The warning went on to say, "*thinking of investing in Bitcoin or other Cryptocurrencies?"* and warned "*scammers will often contact you offering to invest in cryptocurrency (e.g. bitcoin) and will offer to guide you through opening a cryptocurrency account. If you cannot access the cryptocurrency wallet or withdraw money from it, this is a scam and you should stop making payments immediately".* The warning had a link to the FCA's website which gave advice.

NatWest showed us evidence that this message was sent for the first payment, but couldn't confirm what Ms T's response was, nor could they say if the warning was presented on the second payment as well.

I then went onto consider what would've happened if NatWest had contacted Miss T – over and above the warning when the first payment was made. And on balance, here I agree with our investigator. I reviewed Miss T's testimony and:

- She was looking to invest to make money as her line of work had been paused because of the pandemic.
- She had been encouraged to invest in bitcoin by a friend who'd made money.
- She seemed to believe the claim that returns of £7,000 on an investment of £14,000 was possible – even though in many ways this was too good to be true.
- She initiated online research herself into bitcoin investment.
- She carried out due diligence on the investment company A and was content it was genuine. She said the reviews were positive.
- I noted that there were negative reviews on A dating from June 2020, saying the company were a scammer – so if Miss T did see those, she chose to ignore them.
- She said she spoke to several different people at A which gave the impression it had a large and credible company structure.

- The scammer didn't pressurise her to make a payment for some weeks – and she could see the first payment of £2 had been received. She tracked performance on A's website on her account.
- She came to trust the scammer as a friend and advisor. He appeared attentive and professional. He appeared to have her best interest at heart.
- He produced in-depth information about the trading process.

For all these reasons, on balance, I'm persuaded that if NatWest had intervened, Miss T would've decided to go ahead anyway.

And therefore, my decision is that NatWest do not have to refund the money to Miss T.

*Recovery*

We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I looked at whether NatWest took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost funds. But in this case, as the payments were sent to Miss T's own account with B, there was no requirement to do so - as Miss T had then moved the funds onto the bitcoin scam company A.

I'm sorry Miss T has had to contact us in these circumstances. I accept she's been the victim of a cruel scam, and will be disappointed by my decision, but I can't reasonably hold NatWest responsible for her losses.

**My final decision**

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss T to accept or reject my decision before 6 November 2023.

Martin Lord
**Ombudsman**