

The complaint

Mr W is unhappy National Westminster Bank Plc (“NatWest”) won’t refund the money he lost as a result of a third-party scam.

What happened

The circumstances that led to this complaint are well known to both parties, so I won’t repeat them in detail here. But, in summary between 6 October 2022 and 19 October 2022 Mr W made multiple payments totalling £5,990 to an individual I will refer to as S. He also received two credits as part of the scam totalling £400.

Mr W says he found the opportunity to invest on a social media site. He said he saw many endorsements on the site. He also says he spoke with S who advised him he could double his investment with guaranteed results and that he could get back up to £50,000 on a £500 investment. When Mr W asked to withdraw the investment, he was told there were fees and taxes due.

Mr W complained, via a third-party representative, to NatWest in May 2023 that he’d been the victim of a scam and asked it to reimburse the money he’d sent. NatWest declined his claim. It said it provided warnings and the payments were authorised by Mr W. NatWest explained that it contacted Mr W on 20 October 2022 about the credits he’d received (as it received a report from the sender’s bank - who was also a victim of a scam). Due to its concerns over Mr W’s responses, it said it provided Mr W with scam prevention advice at this.

Our investigator did not uphold the complaint. She considered the complaint under the Lending Standards Board’s (LSB) Contingent Reimbursement Model (CRM) Code. But she felt the transactions didn’t necessitate a warning and that Mr W didn’t have a reasonable basis for believing this was a genuine investment opportunity.

Mr W’s representative did not agree with the investigator’s view, so the case has been passed to me for a final decision.

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.

In deciding what’s fair and reasonable, I’m required to take into account relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

Where the evidence is incomplete, inconclusive or contradictory, I reach my decision on the balance of probabilities – in other words, on what I consider is most likely to have happened in light of the available evidence and the wider circumstances.

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 terms and conditions of the customer's account. And I have taken that into account when looking into what is fair and reasonable in this case. But a bank also has to be on the lookout for, and help to prevent payments, that could involve fraud or be the result of a scam.

When considering what is fair and reasonable in this case, I have taken into account the LSB's CRM Code – which NatWest is a voluntary signatory to.

Mr W's representative has referred to new rules coming out later this year – which they feel show the regulatory intent in this area. But I am considering the Code that applied at the time of the transactions and the rules can't be applied retrospectively.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment (APP) scams like this, in all but a limited number of circumstances. One exception is whether:

- Mr W made the payments without a reasonable basis for believing that they were for genuine goods or services; and/or the investment/the person purporting to invest on his behalf was legitimate.

There are other exceptions to reimbursement, but they aren't relevant in this case.

Did Mr W have a reasonable basis for belief?

The phrase 'requisite level of care' was removed from the Code in April 2022. I do agree with Mr W's representative that the CRM Code is not binding on consumers and there is no set standard of care or specific responsibilities placed on customers via the Code. And I have taken into account the LSB's 2022 Review of adherence to the (CRM) Code published in September 2022 when considering this part of the Code. I've also considered the characteristics of the customer together with the complexity/sophistication of the scam.

But I need to consider not just whether Mr W believed he was sending money for an investment, but whether it was reasonable for him to do so. Overall, I don't think Mr W did have a reasonable basis for believing this was a genuine investment opportunity for the following reasons:

- Mr W was making payments to an individual 'S' he came across on social media. He relied on the positive 'reviews' on her social media account before sending her money directly to her personal account.
- The promised returns (of up to £50,000 on a £500 investment) were too good to be true especially in the context of a guaranteed return of initial funds invested.
- S had remote access to Mr W's computer and set up a cryptocurrency account in his name and S also had access to this. Although payments were made directly to S – this seems odd given the setting up of a cryptocurrency account and warranted closer scrutiny.
- Later on, Mr W received some payments from S (although they appeared to come from a personal account in a completely different name) to help him pay for investments and fees, but I don't think it's reasonable of him to consider this is how a genuine investment opportunity would operate.

- Mr W used references for the payments for the investment as either 'family support' or 'car'. It's not clear if he was told to do so by S - but it seems odd not to reference it 'investment' if he believed this to be a genuine investment opportunity.

I don't think this was a particularly sophisticated scam and given this was supposed to be an investment opportunity - I think that Mr W ought to have had greater concerns about the deal and that, in turn, ought to have led to a greater degree of scrutiny.

Overall, I'm not persuaded Mr W had a reasonable basis for believing the payee was the person he was expecting to pay; that the payment was for genuine goods or services; or the person/ business with whom Mr W transacted was legitimate.

Did NatWest meet its obligations under the CRM Code?

The CRM Code says where firms identify APP scam risks in a payment journey, they should take reasonable steps to provide their customers with "effective warnings", which should include appropriate actions for those customers to take to protect themselves from APP scams.

But I don't think this was a scenario where NatWest reasonably ought to have identified a scam risk here. I think it reasonable for NatWest to take into account a range of factors when deciding whether to intervene or provide a warning. I am mindful that banks can't reasonably be involved in every transaction. There is a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments.

The transactions are spread out and the individual payments very low in value - although I appreciate, they were not insignificant to Mr W. Overall I don't think the pattern or value of payments were consistent with a heightened risk of financial harm. So, in the overall circumstances, I don't think NatWest needed to do more before it processed these payments.

That said - I do note NatWest says warnings were given in response to the payment purpose Mr W selected. I haven't considered whether those warnings were 'effective' here – because for the reasons already explained – I don't think this was a scenario that warranted NatWest providing a warning.

NatWest contacted Mr W regarding the credits he'd received *after* he had made the disputed transactions. So it was too late to stop the preceding payments at this point.

Did NatWest do enough to recovery Mr W's funds?

I've also thought about whether NatWest took reasonable steps to recover Mr W's funds once it was made aware he was the victim of a scam. The first scam payment was made on 6 October 2022 and the last on 19 October 2022. The scam was reported in May 2023 but even if NatWest had reached out to the beneficiary bank immediately after Mr W explained about the credits he'd received in October 2022 – I've seen the third-party beneficiary bank statements that show Mr W's money had already been removed. This is not unusual as scammers usually remove funds within hours.

I am sorry Mr W has fallen victim to a scam and suffered a loss, but I don't think it was caused by a failing on NatWest's part.

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 W to accept or reject my decision before 20 June 2024.

Kathryn Milne
Ombudsman