

The complaint

Mrs C complains that National Westminster Bank Plc didn't do enough to protect her from the financial harm caused by an investment scam, or to help her recover the money once she'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

Mrs C was the victim of an investment scam. She came across an investment company which I'll refer to as "S" after seeing it endorsed on social media by a well-known celebrity. She 'liked' the video and was then sent a private message by someone I'll refer to as "the scammer", who claimed to work for S. The scammer didn't specify a rate of return, but he told her she could make money by investing in cryptocurrency.

Mrs C checked S's website and noted it looked legitimate and had a padlock sign on the top of the webpage. There was also a live-chat facility and positive reviews on both the website and social media page.

The scammer instructed Mrs C to open an account with an EMI which I'll refer to as "R" and to first purchase cryptocurrency through a cryptocurrency exchange company which I'll refer to as "C", before transferring the funds to an online wallet. On 3 October 2023, Mrs C paid £1,000 to C via open banking. On 6 October 2023 and 8 October 2023, she transferred £1,050 to "A". And between 10 October 2023 and 20 October 2023, she made seven transfers to her own account with R totalling £3,522.

When she wanted to withdraw her funds, she was told she'd have to pay a fee, so she made a payment from her NatWest account. She realised she'd been scammed when she was asked to pay more fees.

She contacted NatWest, but it refused to refund the money she'd lost, stating it had contacted the beneficiary bank, but no funds remained. It explained that this was an Authorised Push Payment ("APP") scam and when she made the payments, she would have received a warning message asking if the payee was trustworthy. She was also shown a warning which was relevant to purchase scams, before indicating she was happy to proceed. It said it would have expected her to perform more due diligence and that it had acted on her genuine instructions to process the transfers, so it wasn't responsible for her loss.

Mrs C wasn't satisfied and so she complained to this service explaining that NatWest didn't intervene when she made the payments, she didn't have any investment experience, and she wouldn't have gone ahead with the investment if she'd had any doubts.

NatWest further commented that the CRM Code doesn't apply when funds are sent to accounts in the customer's own name. And it wasn't the point of loss, so she should complain to R and C.

It said the first payment was an open banking payment so there wouldn't have been any warning messages, and it wasn't covered under the CRM Code. It accepted the second payment might be covered by the CRM Code, but it argued that Mrs C didn't have a reasonable basis to believe the investment was genuine because she chose to invest in cryptocurrency after seeing a celebrity endorsement on social media, she communicated with the scammer via Telegram and followed instructions to set up accounts with R and C, she was advised the payment was for commission and initially stopped the payment after reading the warning message issued by NatWest, but then actioned it again a few days later. It also said that no legitimate company would use an employee's account to take payments.

Our investigator thought the complaint should be upheld. He told Mrs C that NatWest didn't need to intervene when she made the first payment, because it was low value. He accepted the second payment was caught by the CRM Code, but he was satisfied NatWest had provided an effective warning on 6 October 2023, so he didn't think she was entitled to a refund under the CRM Code. However, he thought NatWest missed an opportunity to stop the scam, and so it should refund the money Mrs C transferred to R between 9 October 2023 and 20 October 2023. But he thought Mrs C ought to have carried out more due diligence, so he recommended the settlement should be reduced by 50% for contributory negligence.

Mrs C asked for her complaint to be reviewed by an Ombudsman, arguing that NatWest should have intervened when she made the first payment on 3 October 2023 and if it had asked why she was making this payment and provided a scam warning, she'd have told it what she was doing.

I reviewed the file and explained to both parties that I was minded to direct that NatWest should refund 50% of the money Mrs C lost from 6 October 2023 (which amounts to £3,042), plus 8% simple interest calculated from the date of each payment. NatWest agreed to settle the complaint on this basis, but having initially agreed to the proposed resolution, Mrs C made further arguments, which I've agreed to consider.

Mrs C has explained that the call handler didn't provide scam education during the call she had with NatWest on 6 October 2023, and had it done so, she'd have ceased all communication with the scammer. Further, it allowed a payment to go through on 8 October 2023 to the same payee without any further intervention or warning.

She has argued that the settlement shouldn't be reduced for contributory negligence because she wasn't negligent. She has also submitted evidence showing the scam was very sophisticated and the trading platform appeared to be genuinely showing her profits.

She has also explained that she had to borrow money for rent from friends and family which lead to stress, anxiety, and depression. This was compounded by the fact NatWest failed to take responsibility for her loss, which made her feel she was to blame and meant she had to go through the lengthy process of complaining to this Service.

Mrs C has described that during a call she had with NatWest on 7 November 2023, the call handler became hostile and asked why she didn't check that S was on the Financial Conduct Authority ("FCA") register, which was embarrassing because she didn't know what the FCA was.

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 satisfied Mrs C 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although she didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of her bank account, Mrs C is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mrs C didn't intend her money to go to scammers, she did authorise the disputed payments. NatWest is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

I've thought about whether NatWest could have done more to prevent the scam from occurring altogether. It ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it did enough when Mrs C tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect NatWest to intervene with a view to protecting her from financial harm due to fraud.

I wouldn't expect NatWest to have intervened when Mrs C made the first payment on 3 October 2023, because it was a relatively low value payment to a legitimate cryptocurrency exchange, and it wasn't covered under the CRM Code because it was a payment to an account in Mrs C's own name.

On 6 October 2023, Mrs C decided not to go ahead with a payment having received a written warning from NatWest. During the call that took place following the warning, Mrs C told the call handler she was concerned about the payment, as well as a payment she made on 3 October 2023. The call handler asked some basic questions about the investment, in response to which Mrs C said she'd found it on social media, there were no third parties, and she had full access to her cryptocurrency account. The call handler warned Mrs C about brokers and asked if she wanted to speak to Customer Services, which she accepted. Unfortunately, there is no recording of that call.

I think the call handler missed an opportunity to ask more probing questions on 6 October 2023 and as Mrs C was seeking advice about a payment she'd already made, I think she'd have been honest about the circumstances, and the scam would have been detected. And, based on the way she responded to the warning she was shown before the call, it's likely she'd have listened to and acted on a tailored warning about cryptocurrency investment scams, and I don't think she'd have made any more payments to the scam. NatWest should therefore refund the money Mrs C lost after the call on 6 October 2023.

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence, and, in the circumstances, I think the settlement should be reduced by 50% for contributory negligence.

Mrs C has argued that this was a sophisticated scam and that she shouldn't be held responsible for the fact she believed the investment was genuine. I'm satisfied she hadn't invested before and so this was an area with which she was unfamiliar. She wouldn't have known the returns were unrealistic or how to check the information she'd been given. I'm also satisfied this unfamiliarity was compounded by the sophisticated nature of the scam, the fact she trusted the scammer, and the fact she believed the trading platform was genuine and was reflecting the fact her investments were doing well.

However, it's clear from the call she had with NatWest on 6 October 2023 that Mrs C had concerns about the investment having received a written warning from NatWest, and even though I've concluded NatWest missed an opportunity to stop the scam at that point, I think Mrs C should have acted on her concerns and done some due diligence before proceeding to make further payments. She also failed to disclose the existence of the scammer during the call on 6 October 2023 and had she done so, I think the scam might have been detected sooner.

Recovery

I don't think there was a realistic prospect of a successful recovery of the funds because Mrs C paid accounts in her own name and moved the funds onwards from there. And by the time she reported the scam, it's likely the funds she transferred to A would have been moved out of the account.

Compensation

Mrs C believes she is entitled to compensation from NatWest, but the main cause for the upset was the scammer who persuaded her to part with her funds. I appreciate she feels she has had to complain to this service, but we wouldn't expect NatWest to compensate her for having rejected her claim. Mrs C has also suggested she was made to feel stupid because she didn't check the FCA register, but I don't think this question was unreasonable. And I haven't found any errors or delays to NatWest's investigation, so I don't think she is entitled to any compensation.

My final decision

My final decision is that National Westminster Bank Plc should:

- refund the money Mrs C lost after the call on 6 October 2023.
- this settlement should be reduced by 50% to reflect contributory negligence.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If National Westminster Bank Plc deducts tax in relation to the interest element of this award it should provide Mrs C with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs C to accept or reject my decision before 9 June 2025.

Carolyn Bonnell
Ombudsman