

The complaint

Mr F complains that National Westminster Bank Plc didn't do enough to protect him from the financial harm caused by an investment scam and that it is holding him liable for a loan he didn't consent to.

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.

In July 2023, Mr F saw an advert for an investment opportunity which was endorsed by a well-known celebrity. The advert suggested he could make good returns by investing in stocks and shares with a company I'll refer to as "B". Mr F googled B and the reviews seemed positive, so he completed an online form. He was then contacted by someone I'll refer to as "the scammer" who claimed to work for B.

Between 24 July 2023 and 1 August 2023, Mr F made eight transfers from NatWest to accounts in his own name with "R" and Bank C totalling £65,000. Early in the scam period, he applied for a loan to fund the investment. He was then told that the funds he'd invested had been seized by the cryptocurrency exchange company as the activity was classed as fraudulent, and that he'd have to pay £20,000 to release them. He told the scammer he couldn't afford to pay this, and she said he could apply for an interest free loan with one of B's sister companies, which he could repay within 14 days using the returns from his investment.

On 25 July 2023, £20,000 was credited into Mr F's account from "Z", which he then transferred to Bank C (an account which he was told to open by the scammer) and then onwards to a cryptocurrency exchange.

On 28 July 2023, Mr F registered for online banking and a further loan was credited into his account from NatWest. This loan was for £17,100, and £5,082.22 was used to settle a previous loan, leaving £12,017.78.

He then received an email stating his funds had been seized again and that he'd have to pay a further £30,000 to release them. Again, the scammer said she'd obtain loans from B's sister companies and on 31 July 2023, two loans for £15,000 each were credited into the account from "N". Mr F paid these funds to Bank C the following day before sending them to the cryptocurrency exchange on the understanding that his money would be released. He realised he'd been scammed when he was told he'd have to pay a further £27,000. He contacted Bank C who advised him he'd been scammed.

Mr F complained to NatWest, but it refused to refund any of the money he'd lost. It explained that he didn't receive a loan confirmation because it was applied for on his device, but he knew about the loan, and he wasn't honest about what the funds were for. It explained that affordability was assessed through its automated decision process where customers are asked to provide details, and a credit search is undertaken to assess their wider finances.

Regarding the payments out of the account, it said Mr F was sending funds to his own account, so there was no loss from NatWest. It said that a payment for £1,000 was declined on 28 July 2023 and he was given a scam warning. He was also given relevant scam advice on 31 July 2023. Additionally, he made two payments in branch on 1 August 2023, having completed a customer protection form confirming he was moving money to his own account and that the payments weren't for cryptocurrency.

Mr F wasn't satisfied and so he complained to this service and our investigator recommended that the complaint should be upheld in part. She noted Mr F had shared details with the scammer and allowed her access to his device through AnyDesk, so she was satisfied he knew about the loan and had consented for the scammer to take the loan out in his name. She was also satisfied he used the loan funds for the scam and had benefitted from some of the funds directly, as they were used to repay an outstanding loan.

She commented that the loan was provided to Mr F in good faith, based on his genuine details, and on the understanding that the funds would be used for home improvements. So, she didn't think she could fairly ask NatWest to write off the principal loan sum.

Our investigator also considered whether the loan was affordable. She explained Mr F had passed NatWest's checking criteria and that information from his credit file was used to verify the income declared on the loan application. However, she thought it ought to have completed an income and expenditure assessment, and had it done so, Mr F's bank statement would have shown this was the third loan he'd applied for in a very short space of time, which would have suggested his finances were stretched. Further, his P60 showed his annual salary for 2023-2024 was less than the sum declared on the loan application. And his credit file showed other financial responsibilities such as loans, a mortgage, and credit cards.

She also reviewed Mr F's expenses for the year before the loan was obtained and noted he didn't have an additional £340.03 a month to repay the loan. So, she concluded the loan wasn't affordable.

Regarding the payments out of the account, our investigator explained the Contingent Reimbursement Model (CRM Code) didn't apply to the payments because Mr F had paid an account in his own name.

She explained most of the payments were done through telephone banking and so Mr F did discuss them with NatWest. On 24 July 2023, he confirmed he was transferring funds to an account in his name and was given a warning about safe account scams and HMRC impersonation scams. He confirmed no one had advised him to lie and acknowledged the scam warning and our investigator was satisfied the warning was proportionate.

On 25 July 2023 and 26 July 2023, Mr F said the payments were for home improvements, and the work hadn't started yet. He was given another warning about impersonation scams and advised that criminals tell victims to lie to their banks. Our investigator felt NatWest could have asked him more questions, but she didn't think this would have uncovered the scam because Mr F had been coached and wasn't being honest the true reason for the payments. So, she didn't think further questioning at this point would have made a difference.

On 28 July 2023, he made a payment of £10,000 through telephone banking. He wasn't asked any questions or given any warnings and our investigator thought NatWest should have done more, but she didn't think this would have made a difference either.

During a further call with NatWest on 31 July 2023, Mr F was asked about the £30,000 loan he'd received into the account and why he was moving the funds. He explained he was

moving the funds to get more interest, and it was for materials for a new roof. He denied having been contacted by anyone about cryptocurrency investments or having been asked to make the payment, and he said the account had been set up for some time. He also denied downloading remote access software. He was then warned: *“what your answers are matching is a massive scam we are seeing, and they are concerned this is a scam. Customers saying things are like home improvements. Scammer/fraudster will contact you and ask you to lie to the bank and change the reason for the payment, but it will be either for crypto investment and they will be telling you that you are making lots of money and asking you to send it to [Bank C]. Or someone will be impersonating the bank and asking you to make the payment.”* Mr F denied this matched his situation, but NatWest declined to process the payment.

Our investigator further commented that as the final two payments were made in branch, NatWest had missed an opportunity to invoke Banking Protocol, and, had it done so, she thought the scam could have been prevented because Mr F wouldn't have been able to show that he was having work done on his house. So, she thought NatWest should refund the money Mr F had lost on 1 August 2023. However, she thought he should share responsibility for his loss because even though he thought the loan would be paid off, he'd told NatWest the loan was for home improvements, and he'd ignored warnings from NatWest and Bank C.

Finally, she explained there was nothing NatWest could have done to recover the funds because they were sent to accounts in Mr F's name, and she didn't think he was entitled to any compensation.

Mr F has asked for his complaint to be reviewed by an Ombudsman.

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.

Having done so, I've reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Mr F has been the victim of a cruel scam. I know he feels strongly about this complaint, and this will come as a disappointment to him, so I'll explain why.

The Loan

Consent

In this case, my first consideration is: did Mr F know this loan was being taken out in his name, or was it done without his knowledge and consent? Having considered this carefully, I think it's most likely the loan was taken out in Mr F's name with his knowledge and consent at the time, and he therefore did consent to the loan agreement.

I'm sorry Mr F was scammed. However, this was the fault of the scammer, not NatWest. I can't see it was Mr F's fault that scammer was able to take out a loan in Mr F's name given the fact he'd allowed her remote access to his device using AnyDesk, the application contained details of his annual income and employment and included his email address, bank account, and phone number. I note Mr F has argued that the address on the loan application was an old address and I accept this is because it was taken from his driving license. But this supports that the scammer was using information provided by Mr F.

Significantly, Mr F has described that the scammer told him a loan would be taken out in his name, albeit with one of B's sister companies, and that he'd be able to repay the loan within 14 days. I accept he believed the loan would be obtained from one of B's sister companies, but he still had knowledge that a loan was being applied for in his name and that it would need to be repaid. He also told Z that he'd known about the loans when he first made contact. So, I'm satisfied he knew about and consented to the loan.

Further, the loan was received into Mr F's genuine account, and he then moved the funds out to the scam, so while the funds were lost, I'm satisfied they were used.

The issue I need to decide here is whether it's fair for NatWest to pursue Mr F for the outstanding amount of the principal loan which it paid to him. I couldn't reasonably ask it to write off the principal loan amounts unless its acts and omissions unfairly resulted in Mr F's loss, and/or I was satisfied this was a fair and reasonable outcome. Consequently, I'm satisfied that Mr F should be held liable for the principal loan sums.

Affordability

This was a loan of £17,100, with monthly repayments of £340.03, repayable over 60 months and I would expect NatWest to assess whether Mr F could sustainably make the repayments.

Even though he passed NatWest's checking criteria and the information from his credit file verified the amount of income stated on the loan application, I agree with our investigator that it shouldn't have granted him the loan. This is because, this was the third loan he had applied for in a few days and his P60 would have showed his annual salary for 2023-2024 was £36,901.77, which is less than the amount declared on the loan application. He also had other financial responsibilities and no disposable income, therefore the monthly repayments weren't affordable. So, NatWest should remove all interest, fees, and charges applied to the loan.

The payments out of the account

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

There's no dispute that this was a scam, but although Mr F didn't intend his money to go to scammers, he 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 ought to have intervened to warn Mr F when he 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 Mr F from financial harm due to fraud.

During a call on 24 July 2023 when Mr F was sending £4,000 to R, he confirmed he was transferring funds to an account in his own name and was given a warning about safe account scams and impersonation scams. He confirmed no one had advised him to lie and acknowledged the scam warning. I've considered whether warning was proportionate to the risk presented by the payment, and I'm satisfied that it was, and that NatWest didn't miss an opportunity to detect the scam.

The following three payments were all done via telephone banking. During the calls, Mr F told NatWest the payments were for home improvements, the work hadn't started, and he was moving the funds to another of his accounts to get more interest. He denied having been contacted by anyone about cryptocurrency investments or having been asked to make the payment, and he said the account had been set up for some time. He also denied downloading remote access software. Across the three calls, Mr F was given another warning about impersonation scams and advised that criminals tell customers to lie to their banks. He was also told that the circumstances of the payment matched a common scam type, including cryptocurrency investment scams.

I agree with our investigator that Mr F ought to have been asked some more probing questions during the calls, but as he'd been coached to lie, I don't think NatWest would have detected the scam. And it's clear he didn't pay any attention to the warnings he was given, so there was little else NatWest could have done to prevent his loss.

However, when Mr F attended the branch on 1 August 2023, if NatWest had acted on its existing suspicions about the account activity and invoked Banking Protocol requiring him to show evidence of the intended use for the funds, I'm satisfied this would likely have uncovered the scam because even though he accepts having been coached to lie, he wouldn't have been able to show evidence that the money would be used for home improvements and the scam would likely have been detected. So, I agree with our investigator that NatWest should refund the final three payments.

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence and, in the circumstances, failed to act reasonably.

Mr F wasn't an experienced investor, but this isn't an excuse for failing to take reasonable care that he wasn't dealing with scammers before allowing them remote access to his device and providing his personal information. I accept this was a sophisticated scam, but he received several relevant warnings from both Bank C and NatWest and yet he continued to mislead NatWest with a view to transferring large amounts of money out of his account without questioning what he was being told to do. So, I think the settlement should be reduced by 50% for contributory negligence.

Recovery

I don't think there was a realistic prospect of a successful recovery because Mr F paid an account in his own name and moved the funds onwards from there.

The Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr F says he's fallen victim to, in all but a limited number of circumstances. But the code didn't apply to these payments because Mr F was paying accounts in his own name.

Compensation

The main cause for the upset was the scammer who persuaded Mr F to part with his funds. I haven't found any errors or delays to NatWest's investigation, so I don't think he is entitled to any compensation.

My final decision

My final decision is that National Westminster Bank Plc should:

- remove all interest, fees and charges applied to the loan.
- agree an affordable repayment plan with Mr F for the outstanding loan amount.
- refund 50% of payments made in branch. As the loss suffered originates from the loans towards which Mr F hasn't made any repayments, this settlement won't include interest.

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F to accept or reject my decision before 7 March 2025.

Carolyn Bonnell
Ombudsman