DRN-4448607

The complaint

Mr R complains that Nationwide Building Society didn't do enough to protect him from the financial harm caused by an investment scam company, or to help him recover the money once he'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.

Mr R holds the Nationwide account in joint names with Miss E. In June 2022, he chose to invest in cryptocurrency, using a cryptocurrency exchange company I'll refer to as "C". While he was using C's app, he saw a pop-up claiming to provide an opportunity to make more money by earning rewards. Mr R clicked on the pop-up and was taken to a live-chat with someone claiming to be a broker.

The broker offered Mr R the opportunity to enter a 'mining pool' where additional profits could be made. He sent him a link to another wallet and said he would need to deposit £50,000 within 11 days. On 18 June 2022, after Mr R had completed the last payment for the reward activity, the broker told him he had triggered the 'double lucky reward' activity and that he would need to make further deposits. Mr R told the broker he didn't want the double reward and that he had no knowledge that it had been triggered. But the broker said that once triggered, the activity couldn't be changed and unless he completed the double reward, he wouldn't be able to withdraw his funds.

Between 13 June 2022 and 7 July 2022, Mr R made 41 transfers from his Nationwide account totalling £175,400. During the scam period he received £23,500 worth of credits into his account. He eventually realised he'd been scammed when he was asked to make further deposits to avoid the account being frozen, and the broker stopped responding to his messages. He complained to Nationwide arguing that even though it did block some payments, the questions he was asked weren't probing or open-ended and it failed to provide a tailored or effective warning.

But Nationwide refused to refund any of the money he'd lost. It explained that when it contacted him, he said he was sending funds to his own cryptocurrency wallet and that it couldn't accept liability for the payments because the money was sent to a cryptocurrency wallet which was under Mr R's control.

Mr R wasn't satisfied and so he complained to this service. He said that if Nationwide had recognised the payments as unusual it would have been able to provide tailored warnings which would have protected him from financial harm. He wanted it to refund the money he'd lost and pay £300 compensation for the distress and inconvenience he'd suffered as a result of the scam, and to indemnify him against any liability for costs.

His representative said Nationwide should have intervened as he made 41 payments to a new payee linked to cryptocurrency within the space of one month, having transferred large sums of money into the account before quickly dispersing it. They said Nationwide should

have intervened when Mr R made the second payment of £4,500 on 13 June 2022 as by this point, £9,000 had debited the account in a single day.

Our investigator thought the complaint should be upheld. She noted Nationwide had contacted Mr R on 25 May 2022 because he made a payment which was blocked by VISA. And there was a further call on 26 May 2022 when he said he was trying to buy cryptocurrency. She commented that Nationwide didn't give any scam warnings or ask any questions about the reason for the payments during those calls, but there was a further call on 26 May 2022 when the activity on the account was discussed in detail.

On 26 May 2022, the call handler said that when there are repeated payments to cryptocurrency platforms, they need to check for scams as people are being coerced into making payments by fake brokers. Mr R said he'd been talking to a few people and was prepared to lose the money. He said no one had been in touch with him, he'd done it all by himself and he'd researched the investment. He confirmed the funds had been received into the cryptocurrency account and re-iterated there was no third party involved and that he could afford to lose the money. He also said he was the only person who had access to the cryptocurrency wallet. Our investigator noted that Nationwide had explained that if anyone contacted him out of the blue in relation to cryptocurrency, it was likely to be scammers and she was satisfied the warning was meaningful as it included information about cryptocurrency scams.

During another call on 30 May 2022, the call handler told Mr R about the increase in scams and referred him to the Financial Conduct Authority ("FCA") website to make sure the investment was genuine. Mr R acknowledged the scam risk and assured the call handler that he wasn't going to give any information away.

In another call on 13 June 2022, Mr R said he was trying to buy cryptocurrency, there was no third party involved and he was doing everything himself. He wasn't given a scam warning, but our investigator didn't think it would have made a difference because when he called Nationwide to report the scam on 15 July 2022, he explained he had firmly believed he was dealing with C, so Nationwide wouldn't have been able to uncover the scam.

Our investigator thought the repeated payments of £4,500 were unusual but based on the interactions Mr R had with Nationwide before and including the first scam payment, and the fact he genuinely thought he was dealing with C, she didn't think an intervention before 20 June 2022 would have made a difference.

But she thought that if it had intervened after that point, it could have made a difference to the outcome. This is because on 18 June 2022, Mr R had become frustrated with the broker at being required to make further deposits to get double rewards, which had been triggered without his knowledge. This was the first time during the scam period that he had felt concerned about what he was being asked to do by the broker and she thought that if Nationwide had intervened after this point, it might have made a difference to the outcome.

She thought Nationwide should have intervened on 21 June 2022, when Mr R made a further payment of £4,500 because he was paying a high-risk merchant and the overall spend was £72,500, which was highly unusual. She thought Nationwide should have asked him about the increase in spending and warned him that issues with cryptocurrency usually arise when victims ask to withdraw funds. Had it done so, she thought that as Mr R was frustrated about the continued requests for further deposits, he'd have told Nationwide what he was being asked to do, which would have revealed the scam.

Because of this, she thought Nationwide should refund the money Mr R had lost from 21 June 2022 onwards, but that the settlement should be reduced by 50% for contributory

negligence because it was clear he'd gone ahead without conducting proper checks. She also noted he had been told on more than one occasion that he wouldn't be asked to pay more funds, but he continued making further payments each time he was asked.

Finally, our investigator said Mr R wasn't entitled to any compensation because the upset was caused by the scammers, and she hadn't seen any errors or delays in Nationwide's investigation. And he wasn't entitled to compensation for legal fees, as our service is free to access.

Nationwide asked for the complaint to be reviewed by an Ombudsman. It has argued that the activity on 21 June 2023 wasn't out of character with other recent activity on the account because between 13 June 2021 and 17 June 2021, the transactions were predominantly for £4,500. And as it had already discussed similar payments with him and had been assured there was no third party involvement, there was no reason to intervene again. It has also said that between 7 February 2022 and 21 June 2022, there were only three payments which didn't involve cryptocurrency, so there was no change in the operation of the account, and it had already provided information for Mr R to consider.

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.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr R says he's fallen victim to, in all but a limited number of circumstances, but the CRM code didn't apply in this case because the payments were to an account in Mr R's own name.

I'm satisfied Mr R '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 R is presumed liable for the loss in the first instance.

It's not in dispute that this was a scam, but although Mr R didn't intend his money to go to scammers, he did authorise the disputed payments. Nationwide 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 Nationwide could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to a genuine cryptocurrency exchange company. However, Nationwide 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 R when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Nationwide to intervene with a view of protecting Mr R from financial harm due to fraud.

I've listened to Mr R's calls with Nationwide on 25 May 2022, 26 May 2022, 30 May 2022, and 13 June 2022. During those calls, he was open in his responses to the questions he was

asked. He explained he was investing in cryptocurrency, there wasn't a third party involved and he was keen for the payments to be approved. Based on what took place during these calls, even though I think payments 2 to 13 were unusual for the account, I don't think it would have made any difference if Nationwide had intervened again during that period. This is because, Mr R genuinely believed he was dealing with C, so there was no way Nationwide could have reasonably uncovered the scam.

After the call on 13 June 2022, Mr R made a further 40 payments to the scam totalling £170,900 without any intervention from Nationwide. It has said it had already discussed similar payments with him and had been assured of no third party involvement, so there was no reason for it to intervene again.

While I accept £4,500 became an established payment amount, Mr R was paying out a large amount of money to a cryptocurrency merchant. And he was suddenly making payments exclusively for cryptocurrency. So, even though Nationwide had previously spoken to him about similar payments, it should reasonably have contacted him again to ask why he was making multiple daily payments for the same amount over such a long period of time. This wasn't the way he normally used the account and the repeated payments suggested he was under pressure to make payments. Therefore, even though C was no longer a new payee, and the amounts were the same as other payments Mr R had recently made, I think it should have contacted him again to ask him why he was using his account in this way.

Had it done so, while he still believed he was dealing with C, I think Mr R would have discussed with the call handler the fact he was being required to make further payments to earn double rewards and that he felt under pressure to avoid losing the profits he'd made. I also think it's likely he'd have mentioned the fact he was making payments in response to a pop-up message he'd received in C's app, and that he had been encouraged to join a mining pool to gain access to additional profits. Had this conversation taken place, I think it would have uncovered the scam.

The call handler could then have provided a tailored scam warning and warned Mr R that there were red flags present. I haven't seen any evidence that he was keen to take risks, so I think he'd have listened to the advice and contacted C to verify the content of the pop-up he'd received in its app, and ultimately chosen not to make any further payments.

Because of this I'm satisfied that Nationwide failed to intervene in circumstances which might have prevented Mr R's loss and so it should refund the money Mr R lost from payment 17 onwards.

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence. I accept Mr R didn't consider that there was a third party involved and that the trading platform through the fraudulent link looked the same as it did when he had been using the genuine platform. But I haven't seen any evidence that he did reasonable due diligence.

It's clear Mr R began to have doubts when he was asked to make further deposits on 18 June 2022 that he didn't plan or expect to make. When he was told he would have to make these payments, he should reasonably have raised concerns with C about what he was being asked to do. And had he done so, it's likely the scam would have come to light. So, I agree the settlement should be reduced by 50% for contributory negligence.

Compensation

Mr R isn't entitled to any compensation or legal costs from Nationwide because the distress and inconvenience Mr R suffered was caused by the scammers.

My final decision

For the reasons I've outlined above, my final decision is that Nationwide Building Society should:

- refund the money Mr R lost from payment 17 onwards.
- 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 Nationwide Building Society deducts tax in relation to the interest element of this award it should provide Miss E and Mr R with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss E and Mr R to accept or reject my decision before 3 January 2024.

Carolyn Bonnell
Ombudsman