

The complaint

Mr H 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.

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 H was told by a relative that he'd made money from an investment opportunity with a company I'll refer to as "B". Before going ahead with the investment, Mr H checked B's website, which looked professional featured an 'about us' section and positive reviews. The relative sent Mr H a link which he followed to create an account. He also joined a WhatsApp going for B's investors.

Mr H was told to first purchase cryptocurrency through a cryptocurrency exchange company and then load the cryptocurrency onto an online wallet. He was told that if he invested £5,000, he would make 5% commission a day, and the more he invested, the more profit he'd make.

He already had an account with a cryptocurrency exchange company and on 18 April 2022, he moved £9,000 from there to the wallet address he was given. Then between 21 February 2022 and 18 May 2022, he made 15 payments to a cryptocurrency exchange totalling £17,215.

After six weeks, he decided to make a withdrawal and was told it would take 72 hours. But when he didn't receive the funds, he contacted the WhatsApp group and was told others had similar experiences, at which point he realised he'd been scammed. He contacted Nationwide who said that because the funds had been sent to an account in his own name, there was nothing it could do to assist him.

Mr H complained to Nationwide with the assistance of a representative. The representative said Nationwide had failed to intervene and provide an effective warning, arguing the first transaction was of substantial value to a new cryptocurrency-related payee, which was unusual when compared to the normal spending on the account. They said this should have raised concerns and it should have contacted Mr H to ask questions around the purpose of the payment, whether he'd done any research, whether he'd checked the FCA register and whether he'd received any withdrawals. And with that information, it should have identified that Mr H was likely falling victim to an elaborate investment scam.

They said Mr H wasn't coached to give false answers, so it's likely he'd have fully explained what he was doing and that everything had originated from a 'broker'. And even though he was sending money to a legitimate cryptocurrency exchange, it should have still provided a scam warning in light of all the information known to banks about the increasing number of scams associated with cryptocurrency.

Nationwide pointed out Mr H had made a total of 15 payments to another cryptocurrency exchange, totalling £15,265.00 from 27th September 2021 to 19th February 2022. And the returns Mr H was promised should have raised concerns as should the fact the broker wasn't authorised by the Financial Conduct Authority ("FCA"). It also said it wasn't reasonable to act on advice from a relative.

Mr H wasn't satisfied and so he complained to this service. He said that even though he'd invested before, he wasn't experienced and had acted in good faith on the information he was given. He didn't feel under pressure, so felt he was acting independently. And he did research B before deciding to go ahead but didn't find any negative reviews. He believes if Nationwide had contacted him and asked some basic questions, it would have realised it was a scam and provided a scam warning.

He said the previous payments to cryptocurrency merchants wasn't for cryptocurrency and the payment of £9,000 was unusual as he hadn't made any payments of that value before, so Nationwide should have intervened at that point.

Our investigator didn't think the complaint should be upheld. She explained the CRM code didn't apply to the payments because they were to an account in Mr H's own name. And she didn't think the payments were particularly suspicious when compared to Mr H's normal account activity, explaining he'd made previous payments for £5000 and £3000, including multiple large payments to a cryptocurrency exchange, so she didn't think the disputed transactions were so unusual that Nationwide ought to have intervened. And there were no warnings about the payee, so it didn't need to flag the payments. She was also satisfied Nationwide did what it could to recover the money, but when it contacted the receiving bank, there were no funds remaining.

Mr H has asked for the complaint to be reviewed by the Ombudsman, arguing £9,000 was unusual because the highest previous expenditure was £5,000.

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

I'm also satisfied Mr H 'authorised' the payments for the purposes of the 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, he is presumed liable for the loss in the first instance.

Not every complaint referred to us and categorised as an investment scam is in fact a scam. Some cases simply involve high-risk unregulated investments that resulted in disappointing returns or losses. Some of these investments may have been promoted using sales methods that were arguably unethical and/or misleading. However, while customers who lost out may

understandably regard such acts or omissions as fraudulent, they do not necessarily meet the high legal threshold or burden of proof for fraud, i.e. dishonestly making a false representation and/or failing to disclose information with the intention of making a gain for himself or of causing loss to another or exposing another to the risk of loss (Fraud Act 2006).

I've carefully considered the circumstances, and I am persuaded the broker was operating as part of a scam. But, although Mr H 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 had an obligation to 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 H 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 to protecting Mr H from financial harm due to fraud.

The payments didn't flag as suspicious on Nationwide's systems. I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr H normally ran his account, and I don't think they were. I've considered the account statement for the months prior to the payments, and I note between 27 September 2021 and 19 February 2022 there were 17 payments to a cryptocurrency exchange company, so it wasn't unusual for Mr H to pay money to a cryptocurrency exchange.

And there were payments for £5,000 on 22 June 2021 and £3,000 on 8 November 2021, so even though £9,000 was more than he'd previously spent, I don't think the difference was great enough for the payments to be deemed unusual considering he'd already used the account for large payments to cryptocurrency exchange companies. So, I don't think Nationwide missed an opportunity to intervene.

Overall, I'm satisfied Nationwide took the correct steps prior to the funds being released – as well as the steps it took after being notified of the potential fraud. But for the reasons I've explained, I don't think Nationwide is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 23 October 2023.

Carolyn Bonnell
Ombudsman