DRN-5422558

The complaint

Mr A complains that Nationwide Building Society didn't do enough to protect him from the financial harm caused by a job scam, 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.

On 4 January 2024, Mr A received a WhatsApp message about a job opportunity from someone I'll refer to as "the scammer". When he expressed an interest, the scammer told him about an opportunity to earn money by reviewing films on a platform which I'll refer to as "R". The job required him to pay for tasks using cryptocurrency and at the end of a set of 20-30 'tasks', he would earn commission, and the original deposits would be returned. The scammer told him that a profit was guaranteed.

The scammer told Mr A to open an account with a cryptocurrency exchange which I'll refer to as K and to first purchase cryptocurrency and then load it onto an online wallet. On 25 January 2024 and 26 January 2024, he made two transfers from Nationwide to K totalling £7,749.

In addition to the transactions from Nationwide, Mr A also made three transfers from W totalling £3,502, nine transfers from Bank H to K totalling £64,278, two transfers from Bank L totalling £19,000, and one debit card payment and 38 transfers from R.

Having completed the necessary tasks, Mr A asked the scammer if he could make a withdrawal and was told he'd need to make further payments. He realised he'd been scammed on 13 April 2024 when he ran out of money, he lost contact with the scammer and was unable to access his funds.

Mr A complained to Nationwide with the assistance of a representative who said it should have intervened on 25 January 2025 when he transferred £4,749 to K because it was a large payment which was out of character for the account.

The representative argued that Mr A had never purchased cryptocurrency or made such frequent payments to new and different recipients, and Nationwide should have been on the lookout for job/task-based scams and asked more robust questions. They said that if it had intervened appropriately, it would have identified that he was falling victim to a scam because he was contacted unexpectedly on WhatsApp, he was asked to open a cryptocurrency account, added to a WhatsApp group with others doing this same job, and required to make deposits to unlock premium tasks to earn commission. In addition, the payments were getting larger and more frequent, he was encouraged to take out loans or borrow from family or friends, he was put under pressure to make payments, he didn't have an employment contract, and he was told he could double his investment.

They also explained that Mr A believed the opportunity was genuine because he had checked R's website and thought it seemed authentic, there had been a lot of media coverage regarding the move to remote work, and he was added to a WhatsApp group with other employees/freelancers.

But Nationwide refused to refund any of the money Mr A had lost. It said Mr A had made the payments to an account in his own name, so the Contingent Reimbursement Model ("CRM") Code didn't apply. It said it intervened before both transactions and Mr A said there was no third-party involvement, he'd opened the account because his brother had been investing, he'd made a profit and was able to make withdrawals, he hadn't been asked to lie, and he opened the account himself. It warned him about the risks associated with cryptocurrency and he confirmed he was happy to go ahead with the payments.

Mr A wasn't satisfied and so he complained to this service with the assistance of his representative, but our investigator didn't think the complaint should be upheld. He noted Nationwide intervened before both payments and asked questions. He was satisfied he was given a detailed cryptocurrency warning, which he ignored, having also given misleading information to Bank H, and he didn't think there was anything else Nationwide could have done to uncover the scam, so he didn't think it was responsible for his loss.

Finally, he explained that Mr A transferred funds to a legitimate cryptocurrency exchange in his name and from there he purchased cryptocurrency and moved it onto a cryptocurrency wallet, so there would have been no funds to recover. And he didn't think he was entitled to any compensation.

Mr A has asked for his complaint to be reviewed by an Ombudsman. His representative has argued that Nationwide should have asked probing questions and shouldn't have taken his answers at face value, knowing that some scams typically involve coaching.

The representative has also argued that Mr A wasn't asked what he was using the cryptocurrency for, and that he was only warned about cryptocurrency investment scams, so the warning didn't resonate. He's commented that it is unreasonable to punish Mr A for not disclosing more than he was asked and as job/task scams are the second most prominent scam type related to cryptocurrency, Nationwide should have provided warnings for job/task scams.

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 A 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.

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

There's no dispute that this was a scam, but although Mr A 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 A 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 A from financial harm due to fraud.

Nationwide intervened before both payments and so I've considered whether the interventions were proportionate to the risk presented by the payments. Both payments were significant amounts to a cryptocurrency merchant and so a proportionate response would have been for Nationwide to have asked Mr A to provide a payment purpose and to give a warning tailored to cryptocurrency scams.

Having considered the interventions, I'm satisfied they were proportionate and that Mr A was asked probing questions in response to which he said there was no third-party involvement, he'd opened the account because his brother had been investing, he'd made a profit and was able to make withdrawals, he hadn't been asked to lie, and he opened the account himself. He was then warned about the risks associated with cryptocurrency and he confirmed he was happy to go ahead.

I'm also satisfied that, based on the information Nationwide had, the warnings it gave were relevant and appropriately tailored to cryptocurrency investment scams. Mr A's representative has suggested that job scams are so common that it should also have warned him about job scams too, but I wouldn't expect it to do this unless it had reasonable grounds to suspect that a job scam might be relevant, which it did not.

Mr A's representative has argued that Mr A wasn't specifically asked why he was purchasing cryptocurrency, but I'm satisfied that he said he was trying to make some money, therefore Nationwide had the information it needed. I'm also satisfied that, if he was being honest, this is the point at which I would reasonably expect him to have explained that he intended to use the cryptocurrency to pay for tasks which he expected to receive a commission on and that his failure to do so prevented Nationwide from detecting the scam and proving a warning about job scams.

Overall, I'm satisfied that Nationwide's interventions were proportionate and that even if it had included a warning about job scams, I don't think it would have made a difference. He clearly trusted that the job was genuine to the extent that he was prepared to mislead his banks in order for the payments to be processed and he ignored the warnings Nationwide did give and went on to make further payments from Bank H and R. So, I don't think it missed an opportunity to prevent the scam.

Recovery

I've thought about whether Nationwide could have done more to recover the card payments when he reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in

such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Nationwide) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mr A).

Mr A's own testimony supports that he used a cryptocurrency exchange to facilitate the transfers. It's only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Mr A's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Nationwide's decision not to raise a chargeback request the cryptocurrency exchange was fair.

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

Compensation

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

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. I'm sorry to hear Mr A has lost money and the effect this has had on him. 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

For the reasons I've outlined above, 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 A to accept or reject my decision before 12 September 2025.

Carolyn Bonnell
Ombudsman