DRN-4369802

The complaint

Mr E 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.

In March 2022 Mr E received a cold call from someone claiming to work for a company I'll refer to as "A". The person (herein referred to as "the scammer") said they could help him to make money from investing in cryptocurrency. They began to communicate via WhatsApp and on the phone, and Mr E was led to believe he could make a 20% return on the investment.

The broker told Mr E to download Anydesk onto his device and to open an account with an electronic money institution I'll refer to as "W", which he did on 18 March 2022. They told him to transfer money from Nationwide to W, and from there, to purchase cryptocurrency through a cryptocurrency exchange I'll refer to as "I", before loading it onto an online wallet.

On 31 May 2022, Mr E received £404,737 from the sale of a house, which was credited to his Nationwide account. The scammer knew about this money and told him he could use it for the investment and that he would have the money back in time for a planned house purchase in September.

Between 18 March 2022 and 30 August 2022, he made 50 transfers to W totalling £449,206. The scammer sent Mr E details for an account on A's trading platform, which allowed him to see his trades. He also received emails confirming he'd purchased the cryptocurrency.

Mr E complained to Nationwide in September 2022, after he checked the trading platform and realised it was empty. He told Nationwide he thought A was a genuine investment company and that if it had done the right checks he wouldn't have gone ahead with the payments.

Nationwide refused to refund any of the money. It accepted Mr E had paid out a significant amount of money in multiple transactions in a short space of time, which was very unusual. But it also said the payments didn't raise concerns as they were to an external account in his own name. It said the payments were to an account Mr E's name, so he hadn't suffered any financial loss from his Nationwide account, and he would therefore need to contact W.

Mr E complained to this service with the assistance of a representative. The representative said Mr E had made multiple large payments in a short space of time and Nationwide should have intervened to make further checks, which would have prevented his loss. They explained Mr E didn't know where the scammers got his number and that he'd complained to W and received some money back. They also explained Mr E finds it difficult to discuss finances as he struggles with his memory.

Our investigator thought the complaint should be upheld, stating Nationwide should have intervened when Mr E paid £9,638 on 30 August 2022. He explained the account had a history of large payments in the 20 months before the scam, but on 29 August 2022, he moved £29,683 in 1 hours and 10 minutes, followed by £38,820 on 30 August 2022 in the space of eleven minutes. So, by the time he made the payment of £9,638, it was the fourth high value payment that day and amounted to £68,503 in less than 24 hours. Our investigator was satisfied this was unusual activity and that Nationwide should have intervened at that point.

He explained Nationwide should have contacted Mr E on 30 August 2022 to ask him questions about the purpose of the payments and whether anyone had told him to make the payments. He said there was no evidence he'd been coached to lie to Nationwide, so he thought it was likely he'd have told it that he was investing in cryptocurrency. And with this information, there would have been sufficient grounds for Nationwide to provide a tailored scam warning, which might have prevented further loss.

W has refunded 50% of Mr E's loss from a slightly earlier point. So, our investigator recommended Nationwide should refund £420,024, less 50%, which was included in the sum he'd already been refunded by W. He also explained this was a sophisticated scam and that Mr E believed he'd get his money back in time to proceed with the sale of his house. So, he didn't think the settlement should be reduced for contributory negligence.

Nationwide has asked for the complaint to be reviewed by an Ombudsman. It has said 'me-to-me' payments aren't covered by the Contingent Reimbursement Model ("CRM") Code and has suggested the onus was on W to intervene because the funds were transferred to the scammer from that account.

It has said the outcome is at odds with our approach to other 'me-to-me' scam cases, where we have said that a payment between customer's accounts didn't cause or give rise to a loss prior to the onward payment to the scammer. It has also said that our investigator has applied the same approach as 'me to me' scam cases involving payments to cryptocurrency merchants, which aren't regulated by the FCA. It has argued that permitting payments to a cryptocurrency exchange has visibility that it is a cryptocurrency transaction, whereas it had no knowledge of the onward payments from W.

It has also argued there was a break in the chain of causation as W could still have prevented Mr E's loss and should be regarded as the operative cause of the loss, which is an established principle of causation. And it has suggested that if the case was decided in court, it would been entitled to seek a full contribution from W.

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.

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

I'm satisfied Mr E '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 based on Mr E's account and the fact there is an FCA warning about A which post-dates the scam, I'm persuaded this was a scam. But, although Mr E 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 also 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 E 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 E 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 E normally ran his account and think they were. I accept all the payments were to a legitimate account Mr E held in his own name, and there would have been no indication that he planned to invest in cryptocurrency. I also accept there was a history of larger payments on the account. But on 29 August 2022 and 30 August 2022, he made seven payments to W in less than 24 hours, which totalled £68,503. And the payment of £9,368 on 30 August 2022 was the fourth payment that day, bringing the cumulative spend that day to £38,820. I'm satisfied this was very unusual activity for the account and so Nationwide ought to have intervened.

Nationwide should have contacted Mr E and asked him why he was making the payments. Based on the fact there's no evidence he'd been told to lie to Nationwide, I'm satisfied he'd have explained he was moving money to W with a view to investing in cryptocurrency. I'd then expect Nationwide to have questioned him around how he learned about the investment and whether there was a third party involved, and if so, how he met the third party. It should also have asked him whether he'd been promised unrealistic returns, whether he'd been told to download remote access software to his device and whether he'd been advised to make an onwards payment from the cryptocurrency exchange.

With the answers to these questions, Nationwide would have been able to identify this was a scam and to have warned Mr E that there were red flags present which indicated this was probably a scam. It could have also provided advice on how to check the investment was genuine including checking the FCA register and looking for negative reviews on Trustpilot.

I'm satisfied that even though Mr E had believed the investment was genuine, he'd have listened to a robust warning from Nationwide. He was using money that he planned to use to buy a house. I haven't seen any evidence that he was keen to take risks with this money and he didn't have a history of high-risk investing, so I think that if he'd had any inkling this was probably a scam, it's likely he have changed his mind about the investment.

Because of this, I think Nationwide missed an opportunity to intervene in circumstances when to do so might have prevented Mr E's loss, and so it should refund the money he lost from when I've said it ought to have intervened (which is £420,024, less the £210,012 W has already refunded).

In reaching this conclusion I've considered the points Nationwide raised in response to our investigator's view. Firstly, it has said that there was a break in the chain of causation, so the onus was on W to intervene because the funds were lost from there to the scammer's account, while the transfers from Nationwide to W didn't give rise to Mr E's loss. I accept the money wasn't lost directly from Mr E's Nationwide account, but I'm satisfied that if it had identified that the pattern of spending was unusual for the account, it could have prevented his loss. So, even though the payment journey meant there was a later opportunity for another business to have done the same thing, this doesn't mean Nationwide didn't have an obligation to protect Mr E when he made the payments.

Nationwide has also said there's a distinction between me-to-me scam cases involving payments to a regulated business and those involving payments to cryptocurrency exchange companies, namely that, in the former, there's no visibility that the transaction involves cryptocurrency and that there is a risk of an onwards payment. I accept the fact Mr E was paying his own account meant the nature of the payment alone wasn't enough to identify he might be at risk, but Nationwide is required to stop payments which are suspicious or unusual to protect customers who might be at risk of fraud, and the fact Mr E wasn't paying a cryptocurrency merchant doesn't excuse it for having failed to do that.

Finally, Nationwide has suggested it would be entitled to seek a full contribution from W if this matter had been decided in a court. But this decision is based on what is fair and reasonable in all the circumstances of the complaint, which may be different to what a court would decide.

Contributory negligence

I accept there's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence but, in the circumstances, I don't think Mr E was to blame for the fact he didn't foresee the risk.

In recent years instances of individuals making large amounts of money by trading in cryptocurrency have been highly publicised to the extent that I don't think it was unreasonable for Mr E to have believed what he was told by the broker in terms of the returns he was told were possible.

He hadn't invested in cryptocurrency before and so this was an area with which he was unfamiliar. He wouldn't have known the returns were unrealistic or how to check the information he'd been given. This unfamiliarity was compounded by the sophisticated nature of the scam, the fact he trusted the broker and the fact he believed the trading platform was genuine and was reflecting the fact his investments were doing well. So, I don't think he can fairly be held responsible for his own loss.

My final decision

My final decision is that Nationwide Building Society should:

- Refund £210,012.
- 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 Mr E with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr E to accept or reject my decision before 24 November 2023.

Carolyn Bonnell
Ombudsman