DRN-4840391

The complaint

Mr F complains that Nationwide Building Society didn't do enough to protect him from the financial harm caused by an investment 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.

Mr F saw an advert on social media for an investment company which I'll refer to as "M". He followed the link to register his interest and was messaged by someone who I'll refer to as "the scammer". The scammer claimed he could make great returns by investing in cryptocurrency.

He researched M and found there were positive reviews on social media and Trustpilot and it was registered with Companies House, so it seemed reputable and there was nothing to suggest it was a scam. Unfortunately, M was a clone of the genuine company.

The scammer appeared professional and knowledgeable and told Mr F he could begin with a small investment, which he paid on 15 June 2022. He asked him to first purchase cryptocurrency through cryptocurrency exchange companies which I'll refer to as "C" and "F" and then load it onto an online wallet. Between 16 June 2022 and 19 June 2022, Mr F made five more payments from his Nationwide account totalling £15,678.36. Four of the payments were made using a debit card and the final one was a faster payment.

Mr F decided he wanted to make a withdrawal when his investment reached £40,000, but he was told he'd have to make a further deposit of £6,000 to unlock the account, at which point he realised he'd been scammed.

He complained to Nationwide, but it refused to refund any of the money he'd lost. It said it wouldn't have intervened in the first three payments because they weren't unusual or suspicious. Its systems alerted on 19 June 2023 when he tried to transfer £8020 to F and Mr F who confirmed he was acting of his own volition and had set up the cryptocurrency wallets and made the transfers himself. He also said there was no third-party involvement, and he was acting independently.

It said Mr F wasn't honest about the true nature of the investment, and it had showed Mr F the correct warning based on the information he gave. It didn't accept it was liable because it was misled about the true nature of the scam.

Mr F wasn't satisfied and so he complained to this service with the assistance of a representative who said that if Nationwide had intervened appropriately, it would have identified that Mr F had found the investment through an advert on social media, the payments were being sent to an unregulated third party through a cryptocurrency exchange and that he was taking financial advice from an unregulated broker.

They explained that Mr F had believed the investment was genuine because he'd seen reviews on Trustpilot, he could see his investment on a trading portal, and he had very little investment experience. Further, he remained in contact with the scammer throughout and he didn't realise the returns were unrealistic.

Nationwide further explained that Mr F had selected 'investment' as the payment purpose and would've seen the following warning: *Be aware of scams. Carry out the following checks to lower the risk of losing your money to a scam. Check the FCA warning list for firms to avoid. Check the FCA register to make sure whoever you're speaking to is authorised or has temporary registration and to compare the contact details you've been given. Try calling the number on the register to check it's a genuine opportunity. Search online for independent reviews and known scams. And check your paperwork for inconsistencies.*

How criminals scam you with investments. Criminals pretend to be genuine investment firms to trick you into investing. They copy a company's name and address, use fake emails and websites, and use genuine employees' names. Criminals set up unregulated firms that look real. Some criminals even pay a return on an investment to get you to invest more. Many cryptocurrency investments aren't regulated - if you're not sure how it works, don't invest.
It maintained he was shown the correct warning, it conducted effective open probing questioning regarding the circumstances of the payment and the payment was released based on the information provided to it by Mr F.

Our investigator didn't think the complaint should be upheld. She explained the Contingent Reimbursement Model (CRM) code doesn't apply to card payments, international transfers, or payments to accounts in the consumer's own name.

She didn't think the first three payments were unusual because the account had history of similar spending including a transfer of £2,156 on 31 January 2022, a transfer of £1,008 on 1 March 2022, and a card payment of £725.55 on 21 April 2022. So, Nationwide didn't need to intervene. But she thought Nationwide ought to have intervened when Mr F made the fourth payment because it was a high value payment to a high-risk merchant, and it represented an increase in spending on the account.

But based on what happened when Nationwide did intervene, she didn't think an intervention before the fourth payment would have made a difference. She explained that when Mr F made the fifth payment, he selected the payment reason as 'investment' and was shown the written warning (which I've included above). She accepted the warning wasn't relevant to the type of scam, but she was satisfied it included useful information about scams and provided advice on due diligence.

She was also satisfied that Nationwide did what she would expect during the call, because the call handler asked open questions and flagged concerns about cryptocurrency scams. She commented that it was unable to detect the scam because Mr F denied the existence of a third party and that he still wanted the payment to be processed after he was told that third-party involvement would mean the investment was a scam.

Finally, she explained the payments were made to Mr F's own cryptocurrency account before being sent to the scammers, so Nationwide wouldn't have been able to recover the funds.

Mr F has asked for the complaint to be reviewed by an Ombudsman. His representative has argued the intervention wasn't sufficient and Nationwide should have placed Mr F's answers under more scrutiny. They've said he should have been challenged around why he chose to invest in cryptocurrency because it isn't easy or recommended to beginners. He should also have been questioned about the expected returns, the research he'd done and his plans for

withdrawal. They've also stated that statements such as 'I'm basically storing a portion for the next time I want to invest, and then, you know, and then I'm gonna move the rest, and then withdraw that' should have raised concern that he didn't understand what he was doing.

The representative has also argued that Mr F should have been offered an alternative time for the call because both him and the call handler had difficulty hearing, the questioning was repeatedly interrupted, and it is unclear whether he heard the questions.

Finally, they have argued that Nationwide knew Mr F was unfamiliar with investing and was vulnerable due to his age, so it should have invoked Banking Protocol.

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 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. Nationwide has said the CRM code didn't apply to card payments or payments to an account in the consumer's own name, and I'm satisfied that's fair.

I've thought about whether Nationwide could have done more to recover Mr F's 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.

Ms F's own testimony supports that he used cryptocurrency exchanges to facilitate the transfers. Its 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 F'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 against the cryptocurrency exchange company was fair.

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

I'm satisfied this was a scam, but although Mr F 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 F 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 F from financial harm due to fraud.

I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr F normally ran his account and I think they were. The first three payments were low value payments to a legitimate cryptocurrency merchant, and the spending wasn't unusual for the account. So, Nationwide didn't need to intervene.

Our investigator thought Nationwide should have intervened when Mr F made the fourth payment of £4,032.75, and I agree with her that even if it had done, based on what happened when it did intervene, it's unlikely an earlier intervention would have made any difference.

When Mr F made the fifth payment of £8,020 on 19 June 2022, he chose 'investment' as the payment purpose and was shown a written warning. I'm satisfied the warning was relevant and proportionate to the risk and that it included advice on due diligence, including checks which might help to detect clone companies.

During the call, Mr F told the call handler he was sending funds to a cryptocurrency merchant to be stored for later use. He said he hadn't received any cold calls and no one else had access to his cryptocurrency account. He said he hadn't been asked to download any unusual software to his device and he wasn't being helped or assisted by a third party or anyone claiming to be a broker. He said he chose to invest in cryptocurrency because he was trying to get ahead of his finances, and it seemed like the easiest option. He said he'd made a withdrawal and he understood that if there was a third party involved then it would be a scam.

I'm satisfied that the call handler asked relevant probing questions and she made it clear that the involvement of a third party would indicate the investment was a scam. I'm also satisfied that Mr F was dishonest about the involvement of the scammer and that this prevented the call handler from detecting the scam.

Mr F's representative has argued that Mr F should have been offered an alternative time to take the call because he was on a train and the call was interrupted, but I'm satisfied both parties were able to follow the call and that it was effective. The representative has also argued that the call handler ought to have scrutinised Mr F's comments around his intention to store to cryptocurrency and his suggestion that it was an easy option. But I don't consider these responses amounted the red flags and I'm satisfied his responses indicated that he understood and was aware of the risk.

Unfortunately, the fact Mr F repeatedly denied the existence of a third party meant the call handler was unable to detect the scam and this meant he wasn't given a tailored warning or advice on additional due diligence. It's clear he'd been coached to lie, and in those circumstances, I don't think there was anything else Nationwide could have done to prevent the scam. And I don't think this was a case where Mr F should have been told to attend the branch.

Because of this, I'm satisfied that Nationwide did enough when it intervened in the fifth payment and the outcome would have been the same if it had done the same when he made the fourth payment. So, even if it should have intervened sooner, I don't think this represented a missed opportunity to have prevented Mr F's loss.

Compensation

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

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.

I'm sorry to hear Mr F 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

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 F to accept or reject my decision before 25 July 2024.

Carolyn Bonnell
Ombudsman