DRN-5354198

The complaint

Mr S complains that Nationwide Building Society won't refund the money he lost when he was the victim of a scam.

What happened

In September 2023, Mr S was looking for an alternative cryptocurrency exchange to the one he had been using previously and came across a group on an instant messaging platform discussing a cryptocurrency investment company. The group recommended a cryptocurrency exchange to him, and he was sent a link to sign up with the exchange.

Mr S also contacted the cryptocurrency investment company the group was discussing and began speaking with them. He was guided through a number of steps he was told were necessary to set up his investment account and help his investment run more smoothly, and was given access to the investment company's platform where he could see the money he was investing and the profit it said he was making. And over the following months, Mr S made a number of payments from his Nationwide account to purchase cryptocurrency – which was then sent on to the investment company.

I've set out the payments Mr S made from his Nationwide account, as well as the credits Nationwide has said he received from the cryptocurrency exchange, on the attached spreadsheet.

Unfortunately, we now know the investment company was a scam. The scam was uncovered after Mr S was told he had to pay a large amount to withdraw the profit he was told he had made. He made the payment but then the company stopped responding to him and he was unable to access the company's platform. Mr S then realised he had been the victim of a scam, reported the payments he had made to Nationwide and asked it to refund the money he had lost.

Nationwide investigated but said the scam hadn't taken place when the money left Mr S's Nationwide, but when it left the cryptocurrency exchange. So it didn't agree to refund the money he had lost. Mr S wasn't satisfied with Nationwide's response, so referred a complaint to our service.

One of our investigators looked at the complaint. They thought the evidence suggested Mr S didn't have control of the cryptocurrency exchange account, so the scam had occurred when the funds left his Nationwide account. They also thought Mr S was vulnerable to this scam, so they recommended Nationwide refund his losses in full. They also said Nationwide should pay Mr S £750 compensation for failures in dealing with his vulnerabilities and his scam claim. Nationwide disagreed with our investigator, so the complaint has been passed to me.

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 agree with our investigator that Nationwide should refund the losses Mr S suffered as a result of this scam, in full. I'll explain why below.

Are the payments Mr S made covered by the CRM code?

I've first considered whether the CRM code applies to all the payments Mr S made as a result of this scam.

I've thought very carefully about this and I think it's a finely balanced matter in this case. But where the evidence available is unclear or inconclusive, I must make my decision on what I think is likely to have happened, based on the evidence I do have.

The Lending Standards Board (LSB)'s Contingent Reimbursement Model (the CRM code) is a voluntary code which Nationwide has signed up to. It sets out a number of circumstances in which firms are required to reimburse customers who have been the victims of certain types of scam. But it only covers payments where a customer paid funds to another person for what they thought were legitimate purposes, but which were in fact fraudulent.

There doesn't appear to be any dispute that Mr S has been the victim of a scam, and that the purpose of the payments was fraudulent. But Nationwide has argued that the payments Mr S made out of his Nationwide account were sent to an account with the cryptocurrency exchange in his own name and that he had control over. So it says they weren't sent to *'another person'* and the CRM code does not apply.

From the evidence I've seen, I agree that the account at the cryptocurrency exchange was in Mr S's own name. We've been sent evidence by the cryptocurrency exchange which shows that the account the payments out of Mr S's Nationwide account went to was in Mr S's name, both when it was opened and when the payments were sent. But this is not the only factor that needs to be considered when determining whether the payments were paid to *'another person'* for the purposes of the CRM code.

In April 2023, the LSB wrote to all firms that had signed up to the CRM code to provide a clarificatory update on this point. This document set out three scenarios that it considered did fall within the scope of the code. Below is one of those scenarios:

> *"An account was opened by or for the customer as a result of social engineering by the scammer. The customer then credits the account at the direction of the scammer in the belief that those funds are secure (for instance, as part of a safe account scam) but the scammer has access to those funds (whether or not the customer is aware). If the customer has been socially engineered, the customer may believe the scammer has a legitimate reason to be able to access their crypto asset account or may have unknowingly shared sufficient details with the scammer to allow them to access the account. In such cases, the customer has, in effect, made a payment to another person for what they believed to be a legitimate purpose, and they have lost control of the funds at the point at which they are transferred to the crypto exchange."*

I appreciate that the circumstances of Mr S's case don't exactly fit this scenario set out by the LSB. But I think there are a number of significant factors which do match what the LSB set out, and so suggest these circumstances should be caught by the code.

The evidence the cryptocurrency exchange has sent our service shows the account the funds were sent to was set up, in Mr S's name, in April 2021. And as Mr S accepts he had been carrying out some activity with cryptocurrencies before he fell victim to this scam, I think it's likely this account was set up by him, legitimately, before his involvement with this scam.

Mr S has said he was sent a link to sign up with the cryptocurrency exchange by someone in the group on the instant messaging platform he was using. I've seen a screenshot of the link he was sent, and it appears the link was to a fake version of the cryptocurrency exchange – rather than to the legitimate exchange. And Mr S says he followed this link to try to sign up with the exchange, not realising or remembering that he had opened an account with it previously.

Nationwide has questioned how the fake link would have allowed the scammers to gain access to Mr S's existing account with the legitimate cryptocurrency exchange – particularly if Mr S had forgotten he had the account. But Mr S has said he uses the same username and password for most accounts, and so likely entered the same details when following the fake link that he would have entered when originally opening the legitimate account. And I think this is a plausible explanation.

I also recognise that it's unusual for scammers to set up a fake cryptocurrency exchange platform, and that scams of this type usually involve a fake investment platform but genuine cryptocurrency being sent by the victim from a genuine cryptocurrency exchange. But, as it was being promoted on an instant messaging platform which tends to be used by people in tech industries, it appears this scam was set up to catch those already involved in cryptocurrency in some way. And so the fake cryptocurrency exchange may have been an effort to phish account details of people who already had cryptocurrency account, or just to make the scam more sophisticated and so catch people who already have some knowledge and understanding of cryptocurrency. In any event, I'm satisfied the link Mr S was sent was to a fake version of the cryptocurrency exchange and so, regardless of the motives for it, this does appear to be what happened here.

After following the link and entering his details, Mr S was told by the investment company that he needed to set up an automatic deposit system on his account, so that any funds he deposited with the cryptocurrency exchange would be automatically forwarded to the company's investment platform. And he says he followed these instructions, which actually involved him setting up email forwarding which meant any emails he received from the genuine cryptocurrency exchange would be forwarded on to the scammers and then deleted from his email account.

Nationwide has also questioned why the scammers would need to do this, and whether not receiving any emails should have been more concerning to Mr S than receiving emails would have been. But, if he'd been told the deposits would be automatically forwarded on, I don't think not receiving emails confirming this would necessarily have been concerning for Mr S. And while I again recognise that it is unusual for scammers to take this step, it could again be an attempt to make the scam more convincing or difficult to uncover.

In any event, from the screenshots Mr S has sent us and the emails he has been able to recover, I'm satisfied the email forwarding was set up on his account – and that the beneficiary of the email forwarding was an email address set up by the scammers and not connected to the legitimate cryptocurrency exchange. Nationwide has not suggested any reason why Mr S would have done this, and I can think of no compelling reason for him to have done so, except at the direction of the scammers as part of an effort by them to conceal the activity on the genuine cryptocurrency exchange account in his name.

After setting up the email forwarding, Mr S was then told by the investment company that his account at the cryptocurrency exchange had been set up incorrectly and so he needed to remove two-factor authentication. He was told to record a video saying he wanted it to be removed and send this to an email address for the genuine cryptocurrency exchange, which he did.

Mr S has sent us copies of emails he has been able to recover from the genuine cryptocurrency exchange, which confirm this process and that it was completed, and that two-factor authentication was removed from his account. Nationwide has argued that the process Mr S followed is not the process that is currently shown on the genuine cryptocurrency exchange's website. But the emails Mr S has sent us copies of appear to be from the genuine exchange, and the process he followed appears to have been the process that was in place at the time – even if it has since been changed.

I've also seen copies of Mr S's communication with the investment company, where it asks him to remove the two-factor authentication. So I'm satisfied the two-factor authentication was removed from Mr S's account with the genuine cryptocurrency exchange and that it was the scam investment company that wanted this to happen. And again, I can think of no compelling reason for him to have done this, except at the direction of the scammers as part of an effort by them to conceal the activity on the genuine cryptocurrency exchange account in his name.

Mr S has also said he had no further involvement in the journey his money took after he made the payments out of his Nationwide account. And he has otherwise been a reliable witness throughout this complaint, he has provided evidence to support various parts of his version of events, and I have no reason to doubt what he has said about this.

I'm therefore satisfied that Mr S was sent a link to a fake cryptocurrency exchange, that the scam investment company could have used this link to gain access to his account with the genuine cryptocurrency exchange, that any emails Mr S received from the genuine cryptocurrency exchange from then on were forwarded to an email address set up by the scammers so that Mr S wouldn't see them and that the scammers arranged for two-factor authentication to be removed from Mr S's account with the genuine cryptocurrency exchange.

Taking all this into account, I think it's likely that the scammers then had access to and control over Mr S's account with the genuine cryptocurrency exchange. Mr S therefore lost control of his funds at the point they were transferred to the cryptocurrency exchange. And as this matches many significant factors of the scenario the LSB set out that it considered did fall within the scope of the CRM code, I think the payments Mr S made here also fall within the scope of the CRM code.

Is Mr S entitled to a refund under the CRM code?

As I explained above, the CRM code requires firms to reimburse customers who have been the victim of authorised push payment scams, like the one Mr S fell victim to, in all but a limited number of circumstances. And it is for the firm to establish that one of those exceptions to reimbursement applies.

The CRM code also requires firms to assess whether a customer was vulnerable to the APP scam they fell victim to at the time it occurred. The relevant sections state:

> *"A Customer is vulnerable to APP scams if it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered.*
>
> *This should be assessed on a case-by-case basis.*

In these circumstances, the Customer should be reimbursed notwithstanding the provisions in R2(1), and whether or not the Firm had previously identified the Customer as vulnerable.

Factors to consider include:

a) *All Customers can be vulnerable to APP scams and vulnerability is dynamic. The reasons for dynamics of vulnerability may include: the personal circumstances of the Customer; the timing and nature of the APP scam itself; the capacity the Customer had to protect themselves; and the impact of the APP scam on that Customer.*

b) *A Customer's personal circumstances which lead to vulnerability are varied, may be temporary or permanent, and may vary in severity over time.*

c) *APP scams may include long-running APP scams or in the moment APP scams.*

d) *The capacity of a Customer to protect themselves includes their knowledge, skills and capability in engaging with financial services and systems, and the effectiveness of tools made available to them by Firms.*

e) *The impact of the APP scam includes the extent to which the Customer is disproportionately affected by the APP scam, both financially and non-financially."*

Mr S has told us he has a number of medical conditions, and personal circumstances, which were affecting him at the time he fell victim to this scam.

He's sent us details of several diagnosis he's received, extracts from his medical records and an analysis prepared by a charity for of one of the conditions. These show the conditions affect his ability to interpret information, concentrate and manage stress. He's also explained his conditions mean he struggles and gets overwhelmed when dealing with anything he doesn't understand straight away, and cause severe memory issues. And he's said some of the medication he's been prescribed for his conditions can negatively impact his cognitive function.

He's also explained he'd been separated from his family and children for some time, and that the emotional strain this and his efforts to rectify this separation had on him only compounded the effects of his medical conditions.

I don't think it's necessary for me to set out the specifics of Mr S's medical conditions and personal circumstances any further, as Nationwide has previously been made aware of them. But I'm satisfied they had a significant and severe impact on both his mental and physical health, and that they were affecting him when the scam occurred.

So I think Mr S was vulnerable and susceptible to this type of scam. I think his perception of the possible risks involved and the steps he could take to address them was significantly and adversely affected by his circumstances at the time.

I therefore think Mr S meets the definition of vulnerable from the CRM code, as I don't think it would be reasonable to expect him to have protected himself against this particular scam. And so I think he should be reimbursed in full, regardless of whether any of the exceptions to reimbursement from the code might apply.

Nationwide should therefore refund the money Mr S lost as a result of this scam, in full.

As I think Nationwide should have accepted Mr S's claim and refunded him under the CRM code, I think it would be fair for it to pay interest on this refund from the date it initially rejected his claim, until the date of settlement.

Should Nationwide have done more to protect Mr S when he tried to make the payments?

In addition to its responsibilities under the CRM code, I think Nationwide should have been monitoring its customers' accounts and looking out for unusual or out of character transactions in an effort to identify where customers were at risk of financial harm from fraud.

But while Mr S made a large number of payments out of his account as a result of this scam, including some for significant amounts, he also had a significant history of genuine cryptocurrency-related payments coming out of this account. In the three years before the scam, he had made a large number of genuine payments to cryptocurrency exchanges – similar to the payments he made as a result of the scam. It wasn't unusual for him to make a number of payments on the same or consecutive days, and the amounts of the genuine payments are similar to those made as a result of the scam.

So I don't think the payments Mr S made as a result of this scam will have looked particularly unusual or out of character to Nationwide, when compared to the previous activity on his account. And so I don't think it was unreasonable that Nationwide didn't identify that he could be at risk of financial harm from fraud as a result of them, or take any further steps before allowing the payments to go through.

And so I don't think anything I would have expected Nationwide to have done at the time would have prevented Mr S making these payments, or that it would be fair to require Nationwide to pay interest on the payments from the date they were made.

Did Nationwide treat Mr S fairly during his claim?

Mr S has also complained about the way Nationwide treated him during his claim. He feels Nationwide's decision to hold him responsible for the payments, it's attitude when speaking to him and its failure to acknowledge his vulnerabilities has had a significant negative impact on him, his circumstances and his future prospects.

And from what I've seen, throughout Mr S's claim Nationwide said it hadn't previously been made aware of his vulnerabilities. And it was only when Mr S carried out a subject access request with Nationwide, was sent copies of call recordings from 2018 and 2019 where he notified it of his vulnerabilities, and these call recordings were then sent back to Nationwide, that it acknowledged it had been made aware. And as Nationwide specifically said in one of the recordings that it would make a note of Mr S's vulnerabilities so that he wouldn't have to have these conversations again, I think this was a serious failing on its part.

I think having to repeat the information about his vulnerabilities, and the lack of faith in Nationwide's processes this failing led to, caused Mr S significant distress and inconvenience throughout his claim.

From the rest of the communication I've seen between it and Mr S during his claim, I also think there are a number of occasions where Nationwide doesn't fully engage with or doesn't understand evidence Mr S has sent it, and either misconstrues or misunderstands things Mr S tells it. This leads to Mr S having to write a number of lengthy responses, or obtain further evidence, to further explain his position. And particularly given his vulnerabilities and the significant time pressure Nationwide knew his circumstances were causing, I think this also caused him significant distress and inconvenience.

I should explain that it is not the role of our service to punish businesses, so any award we make is intended to compensate the consumer for the distress and inconvenience they have been caused – not to punish or penalise a business for failures it has made.

And while, as I explained above, I do think there were a number of failings by Nationwide here and the customer service it provided to Mr S fell below the standard I would expect it to provide, the ultimate and original cause of Mr S's loss and the subsequent circumstances he found himself in was the scammers – not Nationwide. Nationwide did also agree to waive or refund a number of overdraft charges on Mr S's account, in an effort to help him. So while I think better service from Nationwide could have lessened the impact the scam had on Mr S, I don't think it would be fair to hold it responsible for the full impact the scam has had on him.

Taking all this into account, I think the award our investigator recommended of £750 is fair and reasonable compensation for the distress and inconvenience the failings I've explained I think Nationwide made caused to Mr S. And so I think this is a fair award and I think Nationwide should pay this compensation to Mr S as part of the settlement of this complaint.

My final decision

For the reasons set out above, I uphold this complaint and require Nationwide Building Society to:

- Refund Mr S the money he lost as a result of this scam
- Pay Mr S 8% simple interest on this refund, from the date it initially rejected his claim until the date of settlement
- Pay Mr S £750 compensation

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 15 April 2025.

Alan Millward
Ombudsman