## The complaint

Mr R complains that Nationwide Building Society ('Nationwide') hasn't reimbursed his full loss after he fell victim to a scam.

## What happened

Mr R says that he encountered an individual I'll refer to as L in this decision when he advertised his expertise in sports arbitrage on social media. Mr R reached out to L, and this led to a professional collaboration in sports arbitrage which was conducted through messaging platforms. After around a year, L introduced Mr R to an investment opportunity involving cryptocurrency promotion and a code that meant the investment would double. L said that the opportunity was time limited and that he was also investing. The investment would be arranged through a company I'll refer to as B through an agent I'll refer to as S.

Mr R contacted S via a messaging app. S said that the minimum investment was £300, and the maximum was £1,000.

On 4 August 2023 Mr R transferred £700 from his cryptocurrency account to a wallet S gave him the details of. Between then and 22 September 2023 Mr R made around a hundred transactions of between £5 and £1,000 to a cryptocurrency exchange (and then on to wallet address details provided by S) or directly to L. The payments to L were made when Mr R was unable to make further payments from his cryptocurrency account and L agreed to pass funds on to S. The transactions were set out in full in the investigator's view, so I won't repeat them here. Mr R took out multiple loans to fund the investment.

Mr R didn't receive the returns that S promised. Various excuses were given, including that the database wiped, the balance didn't stick, the process stopped part way through, and S forgot to add the lock key.

Mr R realised he was a victim of a scam when returns never materialised and he kept being asked to make further payments. He was also in touch with other victims and established that L pretended to be S to facilitate the scam. He reported what had happened to Nationwide.

Nationwide refunded 50% of all payments from and including the fifth payment Mr R made of £1,000 on 14 August 2023 (after deducting the credits received by Mr R). It said it should have intervened at this point. But Nationwide held Mr R jointly responsible for his loss as it said he didn't take enough steps to check the opportunity was legitimate.

Mr R was unhappy with Nationwide's response and brought a complaint to this service.

*Our investigation so far*

The investigator who considered this complaint didn't recommend that it be upheld. She didn't think any of the payments to Mr R's cryptocurrency account warranted intervention by Nationwide. Nevertheless, Nationwide concluded that it should have intervened from the payment of £1,000 on 14 August 2023, so the investigator considered whether it acted fairly in reimbursing 50% of Mr R's loss. She felt that it had for a number of reasons, including the lack of any documentation or proof that S could generate the promised returns, the implausibility of guaranteed returns of double the amount invested, and the fact Mr R didn't have any reason to trust S after he said the account had been wiped early on.

Turning to the payments to L, the investigator said that Nationwide could fairly rely on the reasonable basis for belief exception in the CRM Code and that Mr R wasn't vulnerable as set out in it. The investigator also said that she didn't think Nationwide needed to provide effective warnings in respect of any of the payments but noted that Nationwide had chosen to reimburse 50% of them.

The investigator noted some additional transactions that hadn't been considered by Nationwide and asked it to reimburse an additional £615.49. Nationwide agreed to this additional payment.

Mr R didn't agree with the investigator's findings and asked for a final decision, so his complaint was passed to me to decide. In summary, Mr R said:

- He is unhappy that he's been held liable for 50% of the loss and said the scam was highly sophisticated including a fake representative (S) and deliberate manipulation.
- The investigator failed to take into account his vulnerability as he has suffered anxiety attacks and depression as a direct result of the scam.
- He contests that Nationwide aren't liable under the CRM Code. Nationwide should have provided effective warnings, and he had a reasonable basis for believing it was a legitimate investment opportunity.

I sent Mr R an email explaining why I thought Nationwide had already reimbursed more than I thought it needed to. I said this for the reasons the investigator set out in her view. Mr R didn't agree and asked me to issue a final decision.

He reiterated his belief it was a sophisticated scam that has had a significant impact on him and said that while the CRM Code may not apply to payments to a cryptocurrency exchange, Nationwide has a wider duty of care to intervene when fraud is suspected. Mr R believes the scam transactions he made were unusual despite previous spending patterns. He said this was because when he engaged in sports arbitrage his transactions were predictable and part of a structured process, and were made with legitimate platforms that offered clear returns. In contrast, the scam payments were characterised by repeated losses and demands for further payments.

Mr R also said that he didn't act negligently but was desperately trying to recover his funds. As the scam progressed, his ability to make rational decisions was compromised. Finally, Mr R said that legitimate cryptocurrency platforms offer similar promotions to the one he was offered by S.

## 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.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

I'm very sorry to hear that Mr R has fallen victim to a cruel scam and of the significant impact this has had on him. I can understand why Mr R feels strongly about his complaint, but banks aren't obliged to reimburse all scam victims in full. Whilst I realise my decision will be hugely disappointing to Mr R, I consider Nationwide has already paid Mr R more than I would award.

*Payments to a cryptocurrency exchange*

The payments Mr R made to a cryptocurrency exchange aren't covered by the CRM Code. This is because the CRM Code only applies to certain types of payment made, in pounds sterling, between accounts based in the U.K. In this case the fraudster received cryptocurrency, so the CRM Code doesn't apply to these payments.

In broad terms, the starting position at law is that a firm like Nationwide is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Service Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

But, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Nationwide should fairly and reasonably:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment;
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving and the different risks these can present to consumers, when deciding whether to intervene.

I need to decide whether Nationwide acted fairly and reasonably in its dealings with Mr R when he made the payments, or whether it should have done more than it did. I have considered the position carefully.

As I've explained above, I consider that as a matter of good practice Nationwide should have been on the lookout for unusual or uncharacteristic transactions. So I've first considered whether the payment requests Mr R made were unusual or uncharacteristic.

Having reviewed Mr R's bank statements in the 12 month period before the scam I'm not persuaded the scam transactions were so unusual that Nationwide should have recognised a heightened risk of harm and taken additional steps before processing them.

The scam transactions ranged from £5 to £1,000 and were spaced out over a period of over a month. Having looked at Mr R's statements there were numerous days on which Mr R made multiple significantly higher value transactions. For example, on 4 May 2023 he made seven individual payments of £1,000 as well as a much larger transaction for £22,000 (and other payments that day). There are so many examples of times when Mr R's spending has significantly exceeded the amounts he paid in the scam, with multiple higher value payments on many days.

There's a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments. Whilst banks have obligations to act in their customers' best interests, they can't reasonably be involved in every transaction. To do so would involve significant disruption to legitimate payments.

Taking all of this into account I don’t think Nationwide needed to intervene and ask Mr R questions about the transactions he was making to the cryptocurrency exchange as, put simply, they didn’t stand out as suspicious. This means that I don’t think Nationwide needed to reimburse anything in respect of these payments. But it has already refunded half of the majority of these transactions.

I would award this amount in circumstances where a firm should have intervened, I think that intervention would have broken the spell and prevented a customer’s loss, and I think the customer should share responsibility for their loss. Even if I thought Nationwide should have intervened, I’m satisfied it has already paid Mr R what I would award.

Mr R says the previous transactions are different because they were predictable, to a legitimate platform and there were returns. I can’t reasonably make this distinction. The scam transactions were to a provider of cryptocurrency but were of much lower value and frequency than previous transactions on Mr R’s account. Mr R also received credits from the cryptocurrency provider.

*Payments to L*

The payments to L are covered by the CRM Code.

Mr R says he should be reimbursed because he was vulnerable so I have considered what the CRM Code says about vulnerability.

The CRM Code says that a customer who was vulnerable when they made an Authorised Push Payment (‘APP’) scam payment should receive a full refund of that payment, regardless of any exceptions set out in it. It states that:

“*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*.”

I’ve thought about what Mr R has said in the context of the CRM Code, and I’m not persuaded that he couldn’t reasonably be expected to have protected himself from the scam. The information Mr R has provided about his vulnerability relates to after the scam, but I need to consider the position when the payments were made. And whilst I appreciate Mr R continued to make payments to recover the funds he’d already lost, I’m not persuaded he was unable to protect himself from the scam he fell victim to. It’s clear from the messages Mr R sent to S that he recognised red flags.

I’ve gone on to consider other provisions of the CRM Code which requires firms to reimburse customers who have been the victims of APP scams like this, in all but a limited number of circumstances. Under the CRM Code, a bank may choose not to reimburse a customer if it can establish that:

- The customer made payments without having a reasonable basis for believing that: the payee was the person the customer was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate.
- The customer ignored what the CRM Code refers to as an “Effective Warning” by failing to take appropriate action in response to such an effective warning.

There are other exceptions that aren’t relevant here.

Taking into account all the circumstances of this case, I think the concerns Nationwide has raised about the legitimacy of the transactions Mr R made are enough to support its position that it may rely on an exception to reimbursement in the CRM Code. I don’t think he had a reasonable basis for believing the person he transacted with was legitimate and will explain why. I should also say that it's the combination of these factors that lead me to reach this conclusion.

- When L introduced the investment opportunity to Mr R there was no evidence of a legitimate scheme that was making money.
- Mr R says he researched B and saw that it offered the promotions S referred to. I have completed some research and can only see a cryptocurrency exchange that doesn't offer any such promotions.
- Cryptocurrency is renowned for being volatile and unpredictable, but Mr R was being offered double returns on any funds invested. This is too good to be true and warranted research.
- Mr R had no reason to trust S. From the beginning the process didn't work and S was very poor at communicating. The database 'wiped' multiple times (six I believe) and the money sent disappeared. There were then multiple excuses like the balance didn't stick, the process stopped part way through, S forgot to add the lock key (twice), the process failed, the process timed out, the process stuck at various points requiring further funds, the withdrawal process stopped, the process completed and then backtracked, maintenance work on the database, problems with the equipment, S was sent home from work because of disruptions in in the country where he lived. The excuses became less and less credible and no returns were provided at any stage.
- It's clear that from early on Mr R had concerns. On 16 August he discussed how things had escalated and on 17 August said that the process didn't work. On 18 August Mr R discussed that he had himself to blame for placing his trust in S. On 19 August Mr R referred to sending money again and then on the final payment it gets wiped, and asked S whether that's how it worked. On 22 August Mr R said to S that something wasn't right and by 30 August he said, "You've scammed us", a sentiment he repeated in subsequent messages. There are other examples, but I won't list them all here. But Mr R continued to make payments.
- On 17 August 2023 Mr R asked S how he'd be reimbursed if it didn't work, and S said he wouldn't be. Later that day S said he could do the process again but couldn't guarantee it would work. There was an element of taking a gamble here.
- Mr R wasn't provided with anything to suggest S worked for the company he said he did or had the skills to make him money and he didn't receive any documentation at all. Genuine investments don't work in this way.

In terms of whether Nationwide met its own standards, the CRM Code says that a firm is required to provide an effective warning where it identifies an APP scam risk. I have set out in the section above why I don't think Nationwide should have recognised a scam risk, meaning that an effective warning was not required.

Under the CRM Code if a firm hasn't breached the standards for firms (and I have said above I don't think Nationwide has) and can fairly rely on an exclusion to reimbursement a customer doesn't receive anything. But Nationwide has refunded 50% of most payments covered by the CRM Code.

The investigator referred to the fact Nationwide had missed some payments when calculating 50% of his loss and asked if Nationwide would pay an additional £615.49 – which it agreed to. Given what I have said above, I don't consider Nationwide is liable for this amount and can't reasonably require it to pay. Mr R may contact Nationwide to see if it still agrees to pay the additional sum the investigator recommended but I am not making an award.

Mr R has referred to the emotional damage the scam has caused. I recognise that in addition to the financial loss, scams often adversely affect emotional and psychological wellbeing. It is the scammer who is responsible for this, and I can only make an award if I think Nationwide has acted unreasonably and exacerbated the harm. I’m not persuaded that is the case here.

Overall, whilst I’m very sorry to hear about this scam and how it has affected Mr R, I think Nationwide has reimbursed much more than I would award - so I’m not asking it to do anything more.

## My final decision

For the reasons stated, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I’m required to ask Mr R to accept or reject my decision before 16 January 2025.

Jay Hadfield
**Ombudsman**