DRN-5594365

The complaint

Ms D complains that Nationwide Building Society (Nationwide) won't refund the money she lost when she fell victim to a job scam. Ms D was initially represented in this complaint, but I'll refer to her as it's her complaint.

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.

Ms D explains that at the time of the scam she was preoccupied and feeling vulnerable due to difficult family and private matters. Also, she was experiencing physical and mental health issues and these impacted on her finances and thinking. In addition, she was unaware of risks associated with cryptocurrency.

Ms D was searching online for remote work and came across a commission-based data optimiser job with fake Company I (with the same name as a legitimate overseas company).

Ms D spoke to X (the scammer) on a messaging app and was informed that the job was completing product reviews, without actually using the product, aimed at boosting search engine optimisation and some products earned greater commission.

After discussing the job and completing a suitability form, she was given access to a fake platform in the name of Company I. Ms D was given a mentor and informed that she would need to deposit her own funds in order to top up her balance to complete time limited sets of tasks.

Ms D paid the scammers by:

- Transferring money from her bank account with Bank L to Nationwide and Bank S.
- Then crediting her accounts with Firm C (a crypto exchange), Firm R (an on-line remittance company which she already held an account with) and Firm T (another on-line remittance company).
- Then transferring funds from Firms C, R and T to the scammers.

Here is a list of the Ms D's transactions:

Payment No.	Date	Time	Payment Type	Credit / Beneficiary	Debits	Credits
n/a – credit*	1/10/24			Credit from Person L		£171.01
n/a – credit*	4/10/24			Credit from Person Z		£123.50
1	4/10/24		Card	Card payment to Firm C	£59.41	
2	4/10/24	11:55	Card	Firm R	£45.84	

3	4/10/24	12:22	Card	Firm R	£49.74	
n/a – credit*	5/10/24			Credit from Person Z		£288.00
4	5/10/24	14:26	Card	Firm R	£286.47	
5	7/10/24	12:21	Card	Firm R	£1,802.99	
6	7/10/24	12:39	Card	Firm R	£1,902.99	
7	7/10/24	12:46	Card	Firm R	£47.99	
8	10/10/24	14.50	Card	Firm R	£1,902.99	
9	10/10/24	14:52	Card	Firm R	£1,902.99	
10	10/10/24	14:55	Card	Firm R	£1,202.99	
11	11/10/24	12:06	Card	Firm R	£1,902.99	
12	11/10/24	12:09	Card	Firm R	£1,099.94	
13	23/10/24	20:07	Card	Firm R	£1,502.99	
Totals					£15,210.32	£2,082.51

* It's unclear from correspondence with Ms D whether the credits she received prior to payment 1 and between payment 3 and 4, were from the scammers. Ms D hasn't confirmed who the credits are from but, considering the dialogue between Ms D and the scammer, the payee names and scammers often pay credits early in a job scam as a tactic to demonstrate that the job is legitimate and entice payments, I also think it more likely than not that that these were credits from the scammers.

Over the course of three weeks Ms D was asked to make an ever-increasing number of deposits to gain access to complete her tasks and access her earnings and funds.

Ms D realised she'd been scammed when she tried to withdraw her account balance and was told that she needed to pay tax before the funds could be released.

Ms D complained to Nationwide seeking a refund of the above payments, as she considered that they should've done more to protect her. Her complaint points included the following:

- The above payments were highly unusual, including multiple high value transactions extremely close together. Considering her banking history, they should've been flagged but there was no intervention at all.
- If Nationwide had intervened and asked effective probing questions, she would've likely realised that she was falling victim to a scam.

Nationwide accepted that they should've '*done more to detect the payments'* from payment number 6, for £1,902.99 and they '*redressed 50% of the payments from this point onwards'*. They also offered £100 compensation '*as more could have been done*'.

However, they also considered Ms D should accept 50% liability as they considered she could've '*done more to prevent the scam'.*

Ms D was dissatisfied with Nationwide's response, so she brought her complaint to our service. However, our investigator considered Nationwide's offer, including the compensation payment, to be fair and reasonable.

As Ms D remains dissatisfied her complaint has been passed to me to look at.

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, my decision is to not uphold this complaint, and I'll explain why.

I should first say that:

- I'm very sorry to hear that Ms D has been the victim of this cruel job scam and lost a significant amount of money here.
- In making my findings, I must consider the evidence that is available to me and use it to decide what I consider is more likely than not to have happened, on balance of probabilities.
- I'm satisfied that the contingent reimbursement model and the APP Scam Reimbursement Rules, introduced by the Payment Systems Regulator in October 2024, for customers who have fallen victim to an APP scam, don't apply here due to the payments being made by card.
- Regarding efforts to recover Ms D's loss. As the payments to the scammer were by card to a crypto exchange and remittance company and then onto the scammer, I don't think Nationwide could've been expected to recover the funds. This is because the goods and service were rendered, and no funds would've remained. Also, chargeback rules don't cover scams.
- The Payment Services Regulations 2017 (PSR) and Consumer Duty are relevant here.

  PSR

  Under the PSR and in accordance with general banking terms and conditions, banks and building societies should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment. There's no dispute that Ms D made the payments here, so they are considered authorised.

  However, in accordance with the law, regulations and good industry practice, a building society should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

  Building Societies do have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions.

  So, I consider Nationwide should fairly and reasonably:

  - Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.
  - Have systems in place to look 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 banks and building societies are generally more familiar with than the average customer.
  - In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in

some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

Consumer Duty

Also, from July 2023 Nationwide had to comply with the Financial Conduct Authority's Consumer Duty which required financial services firms to act to deliver good outcomes for their customers. Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Nationwide was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. Also, look out for signs of vulnerability. However, although Ms D has provided information on being vulnerable, and I empathise with her situation, I can't see that any evidence that, prior to this scam in October 2024, she'd made Nationwide aware of this.

Nationwide accept they should've done more here. Upon reflection they think they should've intervened at an earlier stage. They say payment number 6 for £1,902.99 (see above table) should've been an intervention trigger point.

The dispute here though is about both the intervention point and liability, so I've carefully considered whether:

- This was the right trigger point for one of their agents to probe what Ms D was doing and provide education, warnings and scrutiny to detect a scam and protect her from financial harm.
- An intervention from a Nationwide agent would've more likely than not stopped or unravelled the scam.
- It is fair and reasonable for liability to be shared between Ms D and Nationwide when refunding.

Regarding the right trigger point for one of Nationwide's agents to probe what Ms D was doing and provide education, warnings and scrutiny to detect a scam and protect her from financial harm:

- I don't think payments 1 to 5 should've reasonably been considered as being unusual. I say this for the following reasons:
    - Although Nationwide would've noticed payment number 1 was to a crypto exchange and they haven't confirmed they issued an automated warning about the risk of crypto payments, I don't think this payment should've triggered a human intervention.

      This is because it was a one-off payment for a low amount and not all payments in cryptocurrency will be scam payments. Also, it isn't unusual for consumers to use or invest in cryptocurrency and it is common for them to use crypto exchange companies. In addition, Nationwide process thousands of payments each day and, as mentioned above, they have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm.

      Regarding an automated warning, whether or not one was issued, it would've been for the most prevalent type of scams connected to cryptocurrency payments. However, this would've related to an investment scam and as Ms D was convinced it was a legitimate job and the means to pay her employer, I don't think it would've been meaningful to her and prevented her from making further payments towards the scam.
    - Payment numbers 2, 3 and 4 (for £45.84, £49.74 and £286.47) were also for low amounts and importantly Firm R was an established payee and Ms D had previously made payments to them for similar amounts. So, these wouldn't have

been out of character or looked unusual even though they were processed over two days. Also, Firm R are a remittance service and not a specialist crypto exchange.

- Payment 5 for £1,802.99 was also to Firm R and although it was for a larger amount than Ms D would normally pay them, I don't think it was significantly large or unusual to warrant an intervention bearing in mind it was to an established payee. Also, there was a gap of a couple days between payment 4 and 5.

- However, just 18 minutes after payment 5, Ms D made payment 6 for £1,902.99. This was a similar amount to payment 5 that was higher than Ms D would normally spend with Firm R. So, at this point, due to the same day high spend, I think Nationwide should've seen this as unusual, become concerned about the pattern and put in place an intervention with one of their fraud and scam agents before releasing the payment.

  So, I agree payment number 6 should've triggered a Nationwide intervention, to probe what was going on and give appropriate warnings, and this is the point Nationwide identified they should've done more.

However, I think it more likely than not that an effective human intervention at payment number 6 wouldn't have been effective.

I say this because dialogue between Ms D and the scammer shows that she was very concerned about her banks asking her questions and not accepting her payments (the scammer applied time limit pressure to top up her account and she was worried about her funds). She sought advice from the scammer who suggested evasion tactics of using different accounts and making payments in instalments and there is evidence of multiple same day payments (to both Nationwide and Bank S). Also, Ms D says the scammer advised her to *'tell bank that my family and friends have sent this money for my personal maintenance'.*

In addition, information from Firm T shows that when she set up payments to the scammers, she prevented them from implementing fraud prevention measures. When adding two receivers to her Firm T profile, she was shown a warning for each receiver asking if she knew and trusted them and advised to stop the transfer if unsure, yet she selected *'Yes, continue'.* Furthermore, Ms D didn't take note of an automated warning from Bank S.

So, considering the above, I think it more likely than not that upon any intervention she wouldn't have told Nationwide the real reasons for her payments, and they would've found it difficult to ask probing questions, give appropriate warnings, unravel the scam and prevent Ms D from going ahead with the payments.

I then considered whether it was fair and reasonable for Nationwide to split liability.

In addition, to my consideration that an intervention would've likely been unsuccessful, there's a general principle that consumers must take responsibility for their decisions. With this in mind, I have considered whether Ms D did enough to protect herself from the scam.

Although I recognise how convincing these cruel scammers are and I appreciate the difficulties Ms D was facing, I don't think she did enough. I think she ought reasonably to have had concerns about the legitimacy of the job offered given the high salary for low hours and basic tasks. Also, a requirement to send funds in cryptocurrency to acquire the profits she'd supposedly earned for reviewing products that she had never used. In addition, it was an unsolicited job offer via a messaging service app and not receiving a formal contract should've been seen as very unusual and warranted her to exercise greater caution and do more research. And she was paying much more money to the scammer then she was receiving back.

So, for the above reason I think there was contributory negligence from Ms D. Therefore, I consider it to be fair and reasonable, where Nationwide decide to make a refund payment on a scam, for them to say liability should be shared (from the identified trigger point – payment number 6) where both they and the customer have made errors.

Finally, regarding Nationwide's compensation payment, given that they ought to have prevented some of the loss from occurring, as distress and inconvenience has been caused by the cruel scammer rather than Nationwide, I don't think it would be fair and reasonable to require them to make a compensation payment.

In conclusion, I recognise Ms D has been the victim of a cruel scam and I'm very sorry she's lost this money. I realise the outcome of this complaint will come as a disappointment but, for the reasons I've explained, I think Nationwide acted fairly and reasonably when she complained, so I won't be upholding this complaint and asking them to make any further refund.

My final decision

For the reasons set out above, my final decision is that I'm not upholding this complaint against Nationwide Building Society.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms D to accept or reject my decision before 15 October 2025.

Paul Douglas
Ombudsman