

## **The complaint**

Ms H complains that Nationwide Building Society won't refund money she lost after falling victim to a scam.

## **What happened**

The background to this complaint is well known to both parties so I won't repeat it in detail here. But in summary, and based on the submissions of both parties, I understand it to be as follows.

In February 2021, Ms H was called by somebody claiming to be a police officer. The caller told her that somebody was trying to fraudulently use her account and had bought a high value watch using her bank details. The caller went on to tell Ms H that the fraud originated from Nationwide and that the Police were investigating the matter, but they needed her help to catch the perpetrators. But unknown to her at the time she was talking to a fraudster.

Ms H has said when she first got the call she was concerned and that her first reaction was to go onto her account and check if money had left the account. But she's said she was told not to do this, as it would ruin the operation and, in any event, she was told a block had been put on her account. Nationwide has said its records indicate Ms H did log into her account at the time she was speaking to the fraudster.

While communicating with the fraudster, Ms H has said she messaged her son and a family friend to tell them what was happening. Ms H's son, replying to her message, told her that perhaps she should call him, as he was concerned she 'was being had'. Ms H has said with this the fraudster became angry and told her she wasn't paying attention. She's told us, at this point the fraudster gave her a warrant number and transferred her to '999'. Ms H has told us that '999' came up on her phone and the person she spoke to confirmed the call she'd received was genuine, after which she was transferred back to the fraudster.

The fraudsters told Ms H that she needed to go to a particular bureau de change and withdraw funds in Euros, these would then be collected from her home address by a courier. The reason given for Ms H needing to withdraw cash, was that the person in the bureau de change was in cahoots with Nationwide and it was believed counterfeit notes were being given out. Ms H was told that her whereabouts was being tracked and that she should keep her phone with her while she was in the bureau de change. She's said she was given assurances that she would receive all of her money back from a police account.

Ms H has said she was scared and flustered, but she didn't have any doubt that the caller was legitimate, as she'd checked the warrant number. Believing everything to be genuine she followed the fraudsters instructions and went to withdraw the cash. Ms H has said the fraudsters told her that if she was questioned about the withdrawal, she should explain that the money was for a trip to France. But when she first attempted to make the payment, using her debit card, it was declined. Ms H received a text message from Nationwide about the payment checking that it was genuine. Ms H responded 'Y' to the message.

Ms H then contacted Nationwide and spoke with one of its agents. She explained that she was having difficulty processing the payment. The agent asked Ms H if she'd attempted to make the payment since replying 'Y' to the text message, to which Ms H replied 'no'. The agent then asked Ms H how much the payment was for and suggested that she try it again, with the agent offering to stay on the call while she made the payment. The payment then went through successfully, which was for the value of £6,999.25.

The fraudsters told Ms H that she should bag up the cash, along with her driving licence and bank card and it would be collected by a courier from her home address. Ms H did as instructed and, as arranged, handed the bag over to a courier when they arrived and gave them the agreed password.

Ms H has said the fraudster stayed on the line even after the money had been handed over. But that she exchanged messages with a friend, even though the fraudster had told her not to, and Ms H's friend recognised what was happening and the scam came to light.

Ms H raised the matter with Nationwide, as she didn't think it had questioned her enough before she made the payment. Nationwide issued its final response in April 2021 not upholding the complaint. In summary it didn't consider an error had been made as the system alert was to check it was Ms H that was making the transaction, and Ms H had replied to say it was her. But Nationwide did pay Ms H £100 compensation, by way of an apology for not capturing her email address correctly when handling her claim.

Ms H asked for our service to review the matter. One of our investigators looked into things. In summary she thought the transaction Ms H made looked out of character, in comparison to how she usually ran her account. She thought there was enough going on that Nationwide ought to have been concerned that Ms H may have been at risk of being scammed and it should have asked some further questions before allowing the transaction to be made. Our investigator said the withdrawal of Euros was being made at a time when travel wasn't allowed due to Covid-19 restrictions.

Our investigators view was that if Nationwide had intervened, it would have made a difference and stopped the scam. She said this because, although Ms H had been given a cover story about travelling to France, she didn't consider Ms H would have been able to confidently answer any probing questions from Nationwide, and with this, the spell Ms H was under would have been broken and the scam would have come to light.

Our investigator also considered whether Ms H should bear some responsibility and she thought she could have done more to protect herself. In summary this was because before she made the transaction her son had told her he was concerned she was being had. Our investigator also challenged how it made sense that Ms H needed to withdraw 'Euro's' and hand them over to a courier. Our investigator noted that Ms H had told her that she struggled herself to understand it now and how it made sense - and that Ms H had told Nationwide when reporting the scam that 'when saying it out loud, it 'sounds completely ridiculous'.

Overall our investigator recognised that Ms H had fallen victim to a sophisticated scam and she thought Nationwide had missed an opportunity to discuss the payment with Ms H in more detail, and had it done she thought the payment would have been prevented. But she also thought Ms H should bear some responsibility. In view of this she recommended that Nationwide should refund Ms H 50% of the money she lost, along with interest.

Ms H didn't agree with our investigator's view. In summary she said she hadn't previously heard about scams where people impersonate police officers and she wasn't aware of technology that allowed number spoofing. She added the fraudster had described a member of staff at her local Nationwide who was recognisable to her and named the woman in the

Bureau de Change, who had a name badge with the same name on. She's said that although what she was being asked to do seemed odd, she genuinely believed she had to carry out the instructions and was intimidated by who she believed to be a police officer.

Nationwide also disagreed with our investigator's view. In summary this was because it believed Ms H clearly had concerns about the story given by the fraudsters as she discussed it with her son in the first instance. It also didn't think the story the fraudsters had given Ms H was plausible and she didn't have a reasonable basis to believe it, especially considering her son had told her it sounded like a scam. Nationwide added that Ms H had logged into her internet banking before the transaction and so it would have been clear to her that no funds had been removed from her account and there were no pending payments – so it would have been clear that no watch had been purchased.

It added that the 'Chargeback scheme' protection, for debit card transactions, wouldn't have entitled Ms H to a refund as she had got what she had paid for (i.e. the Euros). Overall it said it couldn't have been expected to prevent the loss. Nationwide said the focus of the conversation it had with Ms H, at the time of the transaction, was to establish who was authorising the transaction – so it wouldn't be fair or reasonable to have expected it to ask probing questions. It also said that even if scam intervention had taken place, it's unlikely the customer would have told the truth, as she believed that she was dealing with the police and that Nationwide were involved. Nationwide said that while the transaction was during a period of COVID restriction you could still travel at the time.

As agreement couldn't be reached the complaint has been passed to me for a decision.

### **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 have reached the same outcome as that of our investigator and for similar reasons.

I'm very aware that I've summarised this complaint briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focussed on what I think is the heart of the matter here. If there's something I've not mentioned, it isn't because I've ignored it. I haven't. I'm satisfied I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as a free alternative to the courts.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

In broad terms, the starting position at law is that a bank is expected to process cash withdrawals that a customer authorises it to make, in accordance with the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case. Both sides accept that this transaction was an authorised withdrawal, even though Ms H was the unwitting victim of a sophisticated scam. Given the terms and conditions of a typical bank account, she is presumed liable for the withdrawals in the first instance.

But that is not the end of the story. Taking into account the 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 anti-money laundering, countering the financing of terrorism, and 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 banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make 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.

The terms and conditions of Ms H's account with Nationwide say;

*When we can refuse to act on your instructions*

*38. We may refuse to make a payment or allow a cash withdrawal (and we won't be responsible for any loss to you) if:*

- a) you haven't met all of the conditions for making a payment in these terms and conditions;*
- b) the instruction is not clear or does not contain all the information we need;*
- c) we reasonably consider that the account details (such as account number, sort code and any reference) which you have provided to us are incorrect or do not sufficiently identify the account into which the payment is to be made;*
- d) our security controls require you to produce additional identification or prevent us carrying out the transaction (for example the payment would exceed any limits we have set) before we can make the payment;*
- e) we reasonably suspect illegal or fraudulent activity;*
- f) we reasonably consider that your account has been or is likely to be misused;*
- g) we reasonably consider there is a security or fraud risk on the device you have used to request the payment through Internet Banking or our Banking app;*
- h) we are ordered to do so by a court;*
- i) we might breach a Law if we allow the transaction; or*
- j) you do not have enough money available to use (including any arranged overdraft limit).*

I've first thought about whether I think Nationwide should have intervened. Nationwide has a difficult balance to strike in how it configures its systems to detect unusual activity or activity that might otherwise indicate a higher than usual risk of fraud. But having reviewed the transaction Ms H made, I'm persuaded that it wasn't typical of how the account was usually run and so, I think it ought to have caused Nationwide to be concerned that Ms H might have been at risk of financial harm.

I say that as from looking at Ms H's account statements in the six months leading up to the scam, I'm persuaded the transaction Ms H made to withdraw cash (foreign currency) using her debit card, wasn't typical of her usual account activity. I say this as Ms H typically uses her account for low value direct debit and card payments and it is not common for Ms H to withdraw cash. There is also only one other larger payment that stands out during this time, but that appears to be for the purchase of premium bonds. So I'm persuaded it's fair and reasonable to say that when Ms H is making a transaction on her card for around £7,000 it is

not typical of how she usually operated her account. There isn't really any disagreement about this point, Nationwide has agreed the amount was high and could be deemed unusual account behaviour and the payment did trigger its detection systems, to the extent that it checked with Ms H whether it was she who was making the payment.

I've set out above what I consider to have been good practice at the time. Further, Nationwide's terms and conditions for the account clearly allows it to prevent the use of the account when it suspects fraudulent activity. Nationwide would have been aware of the prevalence of scams and that it would not always be enough to simply verify that it was their customer making the payment. Whilst I accept Ms H received what she had paid for, in this case the Euros, this doesn't mean that there was no risk of its customer being the victim of fraud.

In my judgment, considering Ms H was making an unusual value transaction, I'm persuaded Nationwide should have done more to satisfy itself that she wasn't at risk of financial harm. I think it ought fairly and reasonably to have stepped in to question the payment, given it represented unusual activity on the account and it should have made enquiries about the purpose of the payment before processing it.

I've thought carefully about what was likely to have happened if Nationwide had asked further, probing, questions at the time this payment was being made and of course I can't know for sure. So I need to decide what I think is more likely than not to have happened. Having done so, I'm currently not persuaded it is more likely than not Ms H would have been able to sufficiently reassure Nationwide she was not the victim of fraud.

Nationwide says that even if it had asked Ms H about the transaction, she wouldn't have told the truth. Ms H has confirmed the fraudster gave her a cover story, should she be asked about the transaction, that she was travelling to France. On the face of it, that could be a plausible reason for withdrawing cash in a foreign currency. But I would still expect Nationwide staff to keep in mind that customers, such as Ms H, may have been given a cover story, as this is a common feature of scams and is something I'm satisfied Nationwide would have been aware of at the time.

I'm persuaded Nationwide could and should have done more, using probing questions to get into the detail and test the purpose of the transaction. In these particular circumstances, for example, it could have asked Ms H; what the transaction was for, why was she withdrawing such a high value of currency and had she considered other, safer methods, of payment.

I'm mindful that Ms H was withdrawing a substantial amount of foreign currency in cash, with a cover story that she was travelling to France, at a time when the country had recently moved into a national lockdown. I don't think this should have been lost on Nationwide and I'm persuaded it would have made Ms H's story seem much less plausible and it ought to have heightened Nationwide's concern that Ms H may have been at risk of financial harm. And aside from any other consideration, I'd expect there to have been some concern about the safety of Ms H carrying this amount of cash with her.

On balance, I think if Nationwide had probed and asked these, or similar questions and spoken to Ms H about the different types of scam and what they look and feel like, I don't think she would have been able to answer persuasively or plausibly when put on the spot. I think it's more likely than not the story Ms H was giving would have unravelled and either Nationwide or Ms H would have realised that something was wrong. I say that particularly as Ms H has indicated she had her own concerns at the start and her son had warned her that he was concerned she was being had. So, overall I think an intervention from Nationwide would have made all the difference.

### **Did Ms H's actions contribute to her loss?**

As I've explained, I think Nationwide could've prevented the loss here. But I also have to consider whether Ms H ought to bear any responsibility for the losses she's incurred too. And, in the particular circumstances of this case, I think she should and so I think I should make a deduction to the award to reflect this.

I understand Ms H felt considerable pressure about following the fraudsters instructions, and she's told us she was stressed and flustered. I also accept that the fraudsters used sophisticated techniques to persuade Ms H to carry out the transaction. Fraudsters know that fear can often have a negative effect on a person's thought process and it can be difficult for consumers to think clearly. The pressure that fraudsters apply can certainly make people take steps that, in the cold light of day, they might not otherwise take.

But, given what I've set out above and the individual circumstances of this case, I can't ignore that Ms H seems to have had some doubt about the legitimacy of what she was being asked to do. I say that as Ms H has told us that the first thing she would have thought of doing, when she was told that a watch has been purchased using her account, would have been to check her account. Ms H has said that she didn't log into her account at the time, because the fraudsters had told her not to log in as it would ruin the investigation. But Nationwide have provided evidence that Ms H's account was accessed at the time Ms H was talking to the fraudsters. It also shows the account was accessed from the same IP address Ms H frequently uses for her genuine banking activity, so I think it's more likely than not that it was Ms H who signed into her account. With this I think Ms H would have been able to see there was no sign of suspicious activity on her account, which ought to have raised her suspicions further.

I'm also mindful that Ms H's son had expressed concern to her that she 'was being had' and asked that she call him. But I've not seen that Ms H called her son to discuss matters and continued to interact with the fraudster. While I do note Ms H has told us the fraudster exerted pressure on her to follow their instructions, Ms H was already in some way going against those instructions by interacting with her son and a friend, but Ms H decided to proceed before speaking with her son.

I appreciate that Ms H is somebody that is respectful of authority. But when considering how the scam was unfolding, it doesn't seem typical that the genuine police would ever ask a member of the public to withdraw large sums of cash (and potentially put themselves in danger) as part of a 'sting' operation. Nor would it be normal to also be asked to hand over a driving licence and bank card to a courier. I also consider the link between Nationwide staff supposedly being 'in' on the fraud and the need to withdraw a substantial sum of cash seems tenuous, which I think is supported by Ms H herself saying that she has been unable to make sense of it, either now and when the scam took place.

I'm mindful, given how convincing fraudsters can be that, in isolation, any of the factors I've set out above may not have been enough to have reasonably prevented Ms H from proceeding. But when considering the specific circumstances of this case and all of the factors in the round, on balance, I think that there was enough going on that Ms H could fairly and reasonably have taken further steps to protect herself.

So in the circumstances, I think Ms H must bear some responsibility for her loss. And I think it would be fair to reduce the refund by 50%.

### **Recovery of funds**

I've also looked into whether Nationwide could have done more to recover Ms H's funds once it was made aware of the scam. But Nationwide's notes show it contacted the other banks the payments were sent to and I don't think Nationwide could have done more to recover Ms H's funds.

### **My final decision**

My final decision is that I uphold this complaint in part and order Nationwide Building Society to;

- Refund Ms H 50% of the money she lost to the fraudsters (being £3,499.63)
- Pay 8% interest on this amount from the date of transaction to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms H to accept or reject my decision before 12 July 2022.

Stephen Wise  
**Ombudsman**