

## **THE COMPLAINT**

Mr G holds/held an account with Nationwide Building Society ("Nationwide").

Mr G's complaint is about Nationwide's refusal to reimburse him money he says he lost due to fraud.

## **WHAT HAPPENED**

The circumstances of this complaint are well known to all parties concerned, so I will not repeat them again here in detail. However, I will provide an overview of events.

Mr G says he has fallen victim to debit card fraud. In short, he contends that payments made using his Nationwide debit card were not consented to by him and therefore were unauthorised transactions.

I do not intend on setting out a detailed list of all the disputed payment transactions given the volume. Instead, I will provide a summary. They appear to be:

- According to Mr G, approximately 200 separate payments amounting to about £20,000 in total.
- Made between approximately 2023 and 2024.
- Debit card payments.
- Made to various merchants such as: Uber Eats, Just Eat, Amazon, Vinted, Depop, Airbnb, etc.
- Ranging between approximately £10 and £200 per transaction.

Mr G disputed the above with Nationwide. When Nationwide refused to reimburse Mr G, he raised a complaint, which he also referred to this Service.

One of our investigators considered the complaint and did not uphold it. As Mr G did not accept the investigator's findings, this matter has been passed to me to make a decision.

## **WHAT I HAVE 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 find that the investigator at first instance was right to reach the conclusion they did. This is for reasons I set out in this decision.

I would like to say at the outset that I have summarised this complaint in far less detail than the parties involved. I want to stress that no discourtesy is intended by this. If there is a submission I have not addressed, it is not because I have ignored the point. It is simply

because my findings focus on what I consider to be the central issues in this complaint.

Further, under section 225 of the Financial Services and Markets Act 2000, I am required to resolve complaints quickly and with minimum formality.

### **Regulatory framework**

The regulations which apply in this matter are the Payment Services Regulations 2017 (“the PSRs”).

### **Authorisation**

Under the PSRs, Nationwide is required to refund any unauthorised payment transactions made from Mr G’s account. Therefore, I must decide on the balance of probabilities, whether the disputed payments in this matter were unauthorised, or authorised by Mr G.

The test for authorisation is twofold.

### **Authentication**

Under the PSRs, Nationwide must prove the disputed payment transactions were authenticated. That is, Nationwide needs to provide technical information which shows that the transactions were made using Mr G’s genuine card and security credentials – for example, the card’s chip being engaged, correct PIN code entered, correct card details used and/or Apple Pay used, etc.

Having considered the technical information Nationwide has provided, I am satisfied the disputed payment transactions were authenticated either by Apple Pay or using Mr G’s card details. This technical information covers the period of approximately December 2023 to September 2024. I think this authentication would, on balance, extend to any period outside of the dates mentioned. I say this because of the payment methods used and the repeat payees which transactions are made to.

### **Consent**

Turning now to the second part of authorisation, consent.

Below are three possible scenarios regarding consent:

- a) Mr G consented to the disputed payment transactions himself. That is, he used his debit card to make the disputed payment transactions.
- b) Mr G provided authority to a third-party to consent to the disputed payment transactions. That is, Mr G provided authority to a third-party to use his debit card to make the disputed payment transactions.
- c) A third-party, without Mr G’s authority, gave consent to the payment transactions. That is, a third-party used Mr G’s debit card to make the disputed payment transactions without his authority.

In scenarios (a) and (b), Mr G authorised the disputed payment transactions, so redress would not be available to him. In scenario (c), Mr G did not authorise the transactions, so redress could potentially be available.

### **Which scenario applies?**

Mr G denies making the disputed transactions himself, and he has not said that he provided authority to a third-party to make them. Therefore, I have reflected on whether it is likely scenario (c) applies in this matter, rather than (a) and/or (b). Having done so, I am not persuaded that it does.

Turning to the Apple Pay transactions first. Mr G says that no one had access to his mobile phone. He also has not given any indication as to how his phone could have been compromised. Given this, I am unable to conclude how a third-party accessed Mr G's mobile phone to make the Apple Pay transactions concerned. Further, Mr G says that his phone was/is protected by facial recognition. This means that even if a third-party was able to obtain Mr G's mobile phone without his knowledge – this would not explain how they would have been able to bypass the facial recognition to access the phone. Further, even if I were to accept a third-party was able to bypass this security measure somehow, I would also need to accept the following. That is, the third-party was able to take Mr G's mobile phone, use it to make the payments concerned, and then return the phone to Mr G – undetected and on several occasions spanning a long period of time. To my mind, this proposition seems improbable.

I should also say that the evidence I have seen shows that Apple Pay has been registered to Mr G's mobile number since 14 January 2022. This is the number that both Nationwide and our Service have on file for Mr G.

Turning to the card transactions. Mr G says that no one had access to his card or card details. He told the investigator, amongst other things, *"I don't even go online to look at my bank statements; nobody touches my cards. I live alone. There's no reason for anyone to touch my card, go near my card ... I don't like even parting with it in a shop."* Again, given this, I am unable to conclude how a third-party would have been able to obtain Mr G's debit card to record its details and then make the payments concerned.

Below are some other factors I have taken into account:

- According to Mr G, the disputed transactions occurred from approximately early 2023, to mid-late 2024 (based on the statements he provided). I find it odd that Mr G did not notice any of these payments during this period. I acknowledge that Mr G says he does not check his statements. However, I would have expected a reasonable person to have noticed the transactions when, at the very least, checking their balance. I say this given the long period these payments went on for, and the fact Mr G says he did not have accounts with the payees concerned at the time.
- Mr G's position, in essence, is that a person unknown to him, made the transactions concerned. Having thought about this, I do not find the behaviour of whomever made the payments to be indicative of an opportunistic fraudster. I say this because:
  - The payments were made over a significantly long period. However, fraudsters tend to drain an account quickly before their transactions are detected.
  - Some of the payments – such as those made to Amazon and Uber Eats – suggest that items would have been delivered to an address. This would be quite a risk for a fraudster to take in terms of being discovered – particularly given the significantly long period the payments were made.

Regarding the last bullet, Mr G has expressed concerns about the address(es) the purchased items would have been sent to. In my view, it is not necessary for me to know the address(es) to be able to establish consent.

I acknowledge that Mr G says he was not in the United Kingdom during the time some of the disputed transactions took place. He says he was on holiday. Because of this, Mr G contends that it could not have been him that made the payments as he, “*cannot be in two places at once*”. From what I can tell, many of the transactions to, for example, Amazon, Uber Eats, Just Eat, etc., would have only required Mr G’s card details or Apple Pay to complete. It follows that Mr G would not have needed to be in the country for the transactions to take place. In any event, it is important to highlight that the payments to the payees in this matter occurred both before and after Mr G was on holiday.

Mr G has alluded to the fact that his card could have been cloned. I see no merit in this submission – particularly given most of the payments in this matter were made via Apple Pay.

Taking all the above factors together, they suggest, on the balance of probabilities, that either scenario (a) or (b) occurred in this matter. Based on the evidence and information before me, I am unable to safely conclude that a third-party without Mr G’s authority made the disputed transactions.

### **Conclusion**

Taking all the above points together, I do not find that Nationwide has done anything wrong in the circumstances of this complaint. Therefore, I will not be directing Nationwide to do anything further.

In my judgment, this is a fair and reasonable outcome in the circumstances of this complaint.

### **Organisations**

Given some of the personal information Mr G has shared with this Service, I am going to set out the names of some organisations he might want to consider contacting (if he has not already):

- Citizens Advice
- National Debtline: Free Debt Advice
- Shelter: The housing and homelessness charity

### **MY FINAL DECISION**

For the reasons set out above, my final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I’m required to ask Mr G to accept or reject my decision before 29 July 2025.

Tony Massiah  
**Ombudsman**