DRN-5764055

The complaint

Mr C complains Nationwide Building Society won't refund him for payments which he says he didn't agree to.

What happened

In the early hours of 13 December 2023, Mr C received a text purporting to be from Nationwide which said a payment had been attempted, using Google Pay, on his Nationwide credit card. He responded to confirm this hadn't been made by him. He then received a message saying he'd receive a call from Nationwide's fraud team shortly, and he may need to install some software which the text referred to as anti-virus software – but which actually allows devices to be remotely accessed. It ended, *"During the call, please provide the Google Pay OTP to prevent fraud and safeguard your funds".* Mr C now believes this was a scam.

Mr C says he then received a call which showed as coming from the number on the back of his Nationwide card, claiming to be the fraud team. And, as he had been led to expect, they asked him to verify the "Google Pay code". I've seen he was sent a verification message by Nationwide at 4:43am, which Mr C has pointed out didn't say not to share the code.

Mr C also says he was using remote access software at this point – so, while he shared the code, the scammers would have been able to see and use it anyway. He's provided a letter, signed by a *"phd licenced computer scientist"* who says she verified that his device was remotely accessed from abroad around 4am on 13 December 2023.

On 21 August 2024, Mr C disputed a series of foreign payments, largely made using Google Pay, taken from his Nationwide credit card; the first on 27 December 2023 and the last on 8 August 2024. He said he hadn't made any of the payments, and Google Pay must have been set up during the scam call.

Nationwide said Mr C was liable as he had shared a code with the scammers and due to how long it took him to report the fraud. It maintained its position after Mr C complained, saying he hadn't agreed to the payments and also flagging some personal circumstances that he says contributed to him believing the scam.

Mr C then referred the matter to our service. Our investigator upheld his complaint. She didn't think the sharing of the code, nor the delay reporting the fraud, gave Nationwide grounds to hold Mr C liable for the payments under the relevant regulations.

Nationwide appealed the investigator's outcome. In summary it says the payments are inconsistent with fraud trends – noting the two-week gap between the scam call and when the first payment was made, and the pattern of small payments being made over a period of months. It said a fraudster wouldn't have waited to start making payments and would have sought to spend as much money as possible as quickly as possible.

I then issued my provisional decision explaining why I wasn't minded to uphold this complaint. In brief, I found Mr C had raised disputes with another firm which suggested he and/or his partner were in the region the payments were made from at the time – and he had also reported falling victim to a very similar scam a few months prior. I also agreed with Nationwide that the disputed activity didn't appear characteristic of fraud. Overall, I wasn't persuaded the payments were more likely unauthorised.

I invited both parties to provide any further comments or evidence they wanted me to consider. Nationwide didn't reply by the deadline I set. Mr C replied that he didn't authorise his partner to use his Nationwide account. He also mentioned some medical issues he and his partner suffer with, and asked what evidence was needed to make me change my decision. I explained that, as an impartial service, we can't advise him on how to build his case – but reiterated the deadline for any final responses. That deadline has now passed and nothing further has been received.

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've decided not to uphold it – for the reasons set out below. These are largely the same reasons I gave in my provisional decision. But I have also considered what Mr C has disclosed about his and his partner's health conditions in response to my provisional findings. While I appreciate this may affect what he is able to provide/recall, without further input on the issues I have laid out below, I still consider it more likely the payments in question were authorised.

Broadly, in line with the Consumer Credit Act 1974, Mr C isn't liable for payments from his Nationwide credit card that he didn't make – unless they were made by someone acting on his behalf and/or someone who acquired possession of the "credit token" with his consent.

Mr C says the payments were made by scammers who tricked him into sharing a Google Pay code, whereas Nationwide disputes this. As there is a disagreement about what happened, I must decide what is more likely based on the information I've been provided.

I've thought carefully about what Mr C has told us. And I have taken into account the evidence he has provided – including screenshots of the scam text he received, as well as the genuine Nationwide code I understand it's accepted was used to set up Google Pay. However, factoring this in, I'm persuaded it's more likely the payments were made by Mr C or someone who he had (effectively) authorised to make payments on his behalf.

Firstly, I'm conscious the evidence Mr C has provided places the scam call at around 4am on the morning of 13 December 2023. I've asked him what he was doing at that time, and whether it struck him as odd that Nationwide would call him so early. While Mr C has replied, he hasn't answered this question. Without his input, I do question the plausibility of him expecting Nationwide to call him at this time.

I'm also aware Mr C has reported falling victim to a similar scam in May 2023 (involving another firm, "B") – so only a matter of months before this one. In the earlier instance, he said he was told to share an Apple Pay code with who he thought was B to safeguard his funds, following which Apple Pay payments were made abroad which Mr C disputes authorising.

Again, I've asked Mr C how this earlier scam impacted his actions in December 2023, or whether he made a connection between the events, but he hasn't answered my questions about this. It does strike me as quite unlikely he would fall victim to such a similar scam only a few months later.

I'm also mindful of the location of the payments Mr C is disputing here. They were made from the same region as the payments Mr C has disputed with B. Additionally, I've seen payments were also made in this region from another account Mr C holds – provided by "R".

Notably, some of the R payments were made during the same period as the Nationwide payments. But they weren't reported as fraudulent. Mr C did dispute some – but on the grounds the merchants hadn't paid agreed refunds and/or hadn't provided the expected goods or services. That included several where he said he and/or his partner were denied boarding to flights departing from the same location as the disputed Nationwide payments in 2024. I've seen Mr C had also previously told R his partner was based in this region.

Given the connections Mr C has to the region the disputed payments were made from, I've asked him if he or his partner were in this area between December 2023 and August 2024. He says it was his partner using his R account during that time; he was hoping to go abroad but was unable to travel due to his health. And that is why some of his claims with R mention both him and his partner; he says the airline agreed he couldn't travel and refunded him.

However, this contradicts the basis of the claims Mr C presented to R – as well as us when he escalated his complaints about them. I've seen a claim on the grounds he was denied access to a flight departing from abroad as he was incorrectly deemed not fit to fly by the airline. I've also seen a similar claim for foreign accommodation in May 2024, saying he was incorrectly denied access due to his health. And he provided a doctor's letter in support of his claim reiterating that he was well enough to access the accommodation but was prevented from doing so.

It's inconsistent that Mr C was denied access to foreign flights and accommodation despite being well enough to travel at the time of these payments (as he told R and us previously) – and that he wasn't well enough to travel abroad at that time (as he has now told me). On balance, I think the evidence suggests it's more likely Mr C did visit the area these payments were made from at some point during the period of the disputed transactions. And it seems an unlikely coincidence that the scammers also happened to operate in the same region.

I also agree with Nationwide that the activity doesn't look typical for fraud. If a scammer had managed to set up a Google Pay token using Mr C's card, I would expect them to try to maximise how much they could steal. Waiting around two weeks to start making payments was risky; Mr C could have realised the call was a scam before then, preventing them from stealing any money.

The first payment was for less than £20. There was then a gap of several days before the next payment was taken. While I appreciate the overall value of the disputed payments exceeds £3,000, this was accrued over months. Several payments were less than £1. Only a handful were over £40 – and most were significantly less. Again, it would seem risky for a scammer, without knowing when Mr C might check his account and spot the fraud, to spend in such small, spread-out increments.

I understand Mr C switched to paperless statements around January 2024, then set up online banking around April 2024 – but didn't check his credit card account until August 2024, around two weeks after the last disputed Google Pay transaction (which had been made frequently up until that point).

The payments stopped when the credit card was approaching the credit limit – but there was over £100 left before it would have been breached. It does seem unlikely to me that, having not checked his account for several months while the payments were happening, Mr C spotted them so soon after the activity stopped. I also can't see why a scammer would have stopped spending until the Google Pay token stopped working; they wouldn't have known when Mr C would spot and report the fraud, or when the credit limit would be reached.

I've also noticed that there were some Google Pay transactions made in the UK. I asked Mr C if he already had Google Pay set up on his own phone for his credit card – and if not, if he had any insight into how these could have been made. He said he hadn't used his credit card at the locations I set out to him, and he thinks he reported all Google Pay transactions to Nationwide. However, that doesn't match the list I have from Nationwide of the payments he disputed.

I therefore can't consider the UK Google Pay payments within this case as part of the loss Mr C is seeking; he would need to raise them with Nationwide directly in the first instance. But I have considered what he has told me about them when determining if Nationwide should refund those payments he has disputed.

If Mr C didn't make any of the Google Pay transactions in the UK, that severely limits the account activity he has pointed to placing him in the UK. It also raises the question of how and why the scammers could have used Google Pay in the UK as well as abroad. And it would seem an odd coincidence that the UK locations where the payments were made were local to Mr C.

I'm also conscious Mr C has told me it was his partner using his R account during this period. He says he wasn't aware of the payments until later. I can't overlook that the payments Mr C is disputing here were made in similar locations, and at similar times, to the payments he says his partner was making from his R account. If Mr C similarly allowed his partner to add his credit card to Google Pay, he would be liable for those payments under the relevant regulations – even if he didn't agree to or have awareness of them.

On balance, I think there are too many factors here which suggest it's more likely these payments were completed by Mr C or someone acting with his authority. As mentioned, I have factored in the evidence he has provided when making this judgment. But in my view, I would still need to accept too many coincidences/unlikely occurrences to conclude the scammers set up Google Pay and made these transactions.

I'd point out one piece of evidence Mr C provided was a letter from a Computer Scientist confirming his phone had been remotely accessed around the time of the scam call. However, the letter doesn't make it particularly clear how this was verified. And when I looked up the Computer Scientist on the website of the university her letter says she is a lecturer for, I found she wasn't listed as a staff member. I asked Mr C if he could provide anything further to verify the letter – and he hasn't. So, I don't think I can place much weight on this letter.

In saying all of this, I am conscious of the circumstances Mr C has disclosed to us, including about his health, which I do think make him vulnerable. I've considered whether these factors could have affected what happened, to the extent that some events which would normally seem improbable might seem more likely. But I don't think his circumstances account for all the factors I have laid out above which lead me to think it's unlikely these payments were made by a scammer.

I appreciate this will be disappointing for Mr C. But having carefully considered all the circumstances, I consider it reasonable that Nationwide has treated the payments he

disputed as authorised. I'm therefore not persuaded it would be fair to direct it to refund him.

My final decision

For the reasons given 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 C to accept or reject my decision before 17 September 2025.

Rachel Loughlin
Ombudsman