

The complaint

Miss S complains £460 was transferred out of her Starling Bank Ltd account using the Nearby payment facility without her authority.

What happened

On 14 August 2023 six payments totalling £460 were made to a third party from Miss S's Starling bank account using the Nearby mobile device payment facility. This same third party also paid Miss S two payment totalling £180 on the same day.

Miss S said she did not authorise any of these payments and has been the victim of fraud. Miss S has confirmed the third party is a friend, however, she said she did not have any contact with this friend on 14 August. She explained she was not on the same Wi-Fi network or close enough for a Bluetooth connection at any point during the day, which is necessary for Starling's Nearby payment system.

Miss S telephoned Starling on 14 August after the payments had been made. She explained she had been the victim of fraud and she hadn't authorised the payments. Miss S said she didn't know how the payments had been made. The adviser Miss S spoke to explained she had several mobile devices registered to her Starling account. Miss S asked how many devices were active on her account, the adviser started to explain how many devices were active, Miss S replied '*serious, I don't have so many devices*'. The adviser then explained they could be old devices. The adviser confirmed the make and model of mobile phone she was currently using, an iPhone 12 and access was subsequently cancelled for all other registered devices. The adviser also explained as he had logged her out of all her other devices it would hopefully stop further payments.

Miss S confirmed her password was not written down anywhere and no-one else should have access to her accounts. Miss S said her iPhone 12 mobile phone was in her hands when these payments were made as she was doing something else with her phone when they went out.

Starling investigated Miss S's complaint and wrote to her. Starling explained it did not think there was evidence to support her claim of fraud, that her login hadn't been compromised and it would therefore not refund her the outstanding balance of £280. Starling explained the evidence suggested payments have been made using an authorised mobile device linked to her account.

Our investigator thought the evidence showed Miss S had authorised the disputed transfers. He explained a trusted mobile device Miss S had authorised had been used to make the transfers and she had said no-one else knew the security details to log into her Starling account.

Miss S rejected our investigators view, maintaining the transfers were fraudulent and she had not authorised them. Her complaint has therefore been passed to me to make a final 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.

Where evidence is incomplete, inconclusive or contradictory, I have to make decisions on the balance of probabilities – that is, what I consider is more likely than not to have happened in light of the available evidence and the wider surrounding circumstances.

I appreciate how strongly Miss S feels about her complaint. Although I may not mention every point raised, I have considered everything but limited my findings to the areas which impact the outcome of the case. No discourtesy is intended by this, it just reflects the informal nature of our service.

The Payment Service Regulations 2017 (PSRs) state consumers are generally liable for payment transactions they've authorised, and businesses will usually be liable for unauthorised transactions. There are exceptions to this rule which I will discuss later. Where a consumer denies having authorised a payment transaction, it is for the payment service provider (the business) to prove that the payment transaction was authorised.

Starling provided a list of transactions between Miss S and her friend. In July and August Miss S made a total of 14 payments from her Starling account to her friend by Nearby payments and she received two payments back. It's therefore clear Miss S was monitoring her Starling account, and had accessed and legitimately used the Nearby payment method to the same third party around a similar time period to the disputed transfers.

The evidence I have considered from Starling shows two mobile phones were used to access Miss S's Starling account on 14 August when the disputed transactions occurred. The two phones were an iPhone 12 and an iPhone 6. Starling has explained it is not able to say which device made the disputed transactions as this is not recorded by their systems for Nearby payments. Therefore, the payments could have been made by either the iPhone 6 or the iPhone 12, or a combination of both devices, as both devices were actively being used on Miss S's account on that day.

Starling has provided evidence that each device was registered and authorised by Miss S, this includes a video taken from each of the devices of Miss S's face during setting them up on the Starling app.

Dealing with the iPhone 12 first. Miss S has been clear and consistent this phone remained in her possession throughout the transactions and she has explained no-one else had access to it. This phone was still in her possession when she raised the complaint with Starling. If this phone was used for the transactions, then, as there does not appear to have been any potential compromise of this phone, I would not be able to find transactions from this phone were unauthorised.

I now move on to the iPhone 6. I asked Miss S where the iPhone 6 was on 14 August and if she had access to it and if she had used this registered device to access her account. Miss S responded by saying *'I had two devices but I didn't use 6s for a long time then I lost it... I have no memory what I done with that [sic]'*. Miss S said she could not be definitive about the dates the iPhone 6 device was last in her possession.

I further asked Miss S to account for the several other devices which were active on her account when these transactions occurred, explaining to her the details of each of these devices and asked her to explain what had happened to them. She did not explain how

these devices were activated, or where they were and said in response to my question they were 'lost'.

Section 72 of the PSRs says customers must notify the payment service provider without undue delay on becoming aware of the loss, theft, or unauthorised use of a payment instrument, such as a mobile phone. It also says customers should take all reasonable steps to keep personalised security credentials related to a payment instrument safe. Section 77 of the PSRs say if a customer fails to comply with Section 72, then the bank might not be liable for the payment as this could be considered grossly negligent.

I have considered all of the possible options for how these payments could have been made. Having done so, I think on balance, the most likely explanation is a third party had access to Miss S's iPhone 6 and Starling app and made these payments. I am persuaded this is likely the case because Miss S was unable to account for this device, or the numerous other devices authorised on her account. I asked Miss S if she had deleted her Starling app from the various phones linked to her account before disposing of them, she replied 'no'. I now need to consider whether Miss S should be liable for these payments or whether Starling should refund them.

I have considered carefully the evidence and what Miss S said about the iPhone 6 and the other authorised devices. I think the evidence I have seen shows Miss S either did not comply with the requirement to notify Starling she had lost this device, or that she disposed of it some other way without restricting access to her Starling bank facilities on it. I think on balance, this is the most likely explanation for how these transactions occurred as even if the iPhone 6 had been stolen or found, this would not account for how the third party was able to access her phone and login to her Starling app.

Therefore, I do not think Starling should be held liable for these transactions, I will explain why. I think, whoever made the transactions had access to Miss S's iPhone 6, she appears from the evidence I have seen, to have lost and not reported a payment instrument as missing for some time. Having carefully considered the responses to the questions our service has asked, I think Miss S has been vague about where and how this iPhone 6 was disposed of and think, on balance, it is possible a third party may have obtained it from Miss S with access to her banking app.

This is supported by the fact there are a series of mobile phones over a short period of time. Miss S did not explain to me when asked why and how this had occurred, which I think demonstrates some element of gross negligence on her part by authorising and being unable to account for several authorised devices.

These devices were only deactivated when she contacted Starling about these disputed transactions, this information is important. It persuades me Miss S had not taken reasonable steps to cancel a series of lost or otherwise registered devices in a relatively short period of time.

Because of this I think there is evidence, on balance, Miss S may have lost, used or otherwise disposed of a series of authorised mobile phones without removing her Starling banking details from them or reporting the phones as lost or stolen to Starling, including the iPhone 6 in question.

Moving on to what constitutes gross negligence in more detail, there is no singular definition of gross negligence within civil law and it is often for the Courts to decide the threshold and whether the acts or omissions has breached that determined threshold based on the specific circumstances of the case.

For the purposes of this decision I am satisfied gross negligence can be defined as:

- An act or omission to exercise reasonable care in performing or failing to perform an obligation where such party demonstrates indifference to, or a serious disregard for a reasonably foreseeable risk.

In other words, doing or failing to do something which they reasonably ought to, to avoid a reasonably foreseeable risk.

I have carefully considered the evidence and having done so I think the risk was reasonably foreseeable and Miss S failed to take action and I therefore think this meets the threshold for gross negligent. Miss S could have notified Starling about the active devices she no longer had in her possession at any point, including the iPhone 6 if and when she had lost it. If she had given this device to someone else and provided the login access, she could have ensured the banking app was deleted.

As I have explained, in either of these scenarios, I do not think Starling should be held liable for these transactions for the reasons I have given above.

I appreciate my decision will be disappointing to Miss S, I hope I have explained my rationale and note that no further issues have been reported to our service since the mobile devices were de-registered from her account.

My final decision

For the reasons I have given, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss S to accept or reject my decision before 20 August 2024.

Gareth Jones
Ombudsman