DRN-4728300

The complaint

Mr S has complained that Starling Bank Limited won't refund him for a transaction he says he didn't make or authorise totalling just over £900.

Mr S is also unhappy with the way Starling managed his data subject access request.

What happened

Mr S had a current account with Starling.

On 10 June 2022, an online card payment was made for a hotel booking, using a well-known hotel booking site, I will call B. The transaction was authenticated via Mr S's banking app on his mobile phone.

Mr S says he became aware of the transaction after checking his account statements whilst Starling completed a review of his account in July/August 2023.

On 7 August 2023, Mr S told Starling that he hadn't made the payment to B and said he hadn't raised this sooner due to him suffering with prolonged ill health. Mr S told Starling that he didn't recall making the payment and may not have had his mobile phone with him at the time. And his phone was protected with a PIN, which he never shared with anyone, but that the banking app remained logged in at all times on his phone.

Mr S said that he hadn't disclosed his online banking details, or security credentials needed to access his bank account. Mr S said his banking app was protected by a PIN, which was the same as the one he used for his mobile phone. He also said that he hadn't lost his bank card.

Mr S has explained that due to his ill health he has been confined to his home and that travel hasn't been possible for him for several years. He said he leaves his home with the support of his family to attend medical appointments. So, he says because of his circumstances, he has never used B to book a hotel. Mr S also said he may not have had his mobile phone at the time of the transaction because he lost it. He said he replaced his phone, with exactly the same model as the phone he used to access his bank account.

Mr S also said that Starling hadn't dealt with his data subject access request (DSAR) fairly because it hadn't sent him the information he requested via post. And said it was only able to do so via email. Mr S said this was a breach of data protection law and the Equality Act 2010.

Starling looked into Mr S's fraud claim and decided not to refund the disputed transaction. In summary the bank said:

- The IP address used at the time to authenticate the disputed card transaction matched undisputed transactions Mr S had made

- The transaction was authenticated via a notification in the mobile banking app that was confirmed using Mr S's registered mobile banking device
- Mr S's registered mobile device was used to make undisputed transactions before and after the disputed transaction
- No other mobile device was registered with the banking app
- As a digital bank it had opted to use email to respond to DSAR's as this was a more secure method of sending sensitive information.

Mr S wasn't happy with the bank's response. So, he brought his complaint to our service. He maintained he never made the transaction to B. He wants Starling to refund him the transaction. And pay him compensation for the trouble and upset the matter has caused him.

One of our investigator's looked into Mr S's complaint. She asked Mr S some more questions about what had happened. Mr S maintained that he never made the transaction to B and that his account wasn't protected by biometrics as Starling had suggested which meant the payment would have had to have been approved via the Starling banking app using either a passcode, fingerprint ID or facial ID. He also confirmed he'd made other transactions from his account, around the same time as the disputed payment, which included payments for public transport. And said that he may have replaced his mobile phone around the time of the disputed transaction with an exact model he'd previously used.

The investigator didn't uphold Mr S's complaint. She said that the evidence showed that Mr S's registered mobile phone had been used to authorise the disputed transaction. And his genuine card details had been used to initiate the transaction. She said there was no plausible explanation for how someone would be able to access Mr S's bank card details and mobile device which was used to make the payment to B. So, based on everything, she said Mr S had more likely than not authorised the disputed transaction.

The investigator also said that Starling hadn't done anything wrong in not complying with Mr S's DSAR via the post and wanting to use email.

Mr S disagreed with what the investigator said. He maintained that he didn't carry out the transaction and said Starling should have refunded him when he reported the matter. Mr S said that Starling have failed to prove he made the transaction. He also said that Starling should have responded to his DSAR via post and its failure to do so breached the requirements of data protection legislation and the Equality Act 2010.

As no agreement could be reached the matter has come to me to decide.

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.

Disputed payment to B

There are regulations which govern disputed transactions. Generally speaking, if the evidence suggests its more likely than not that Mr S authorised the payment, Starling is entitled to hold him liable for the disputed transaction. The relevant regulations, to this effect, are the Payment Services Regulations 2017 (the PSRs 2017).

The PSRs 2017 say a payment transaction is regarded as authorised if the payer has given consent to the execution of the payment transaction. If a payment service user (customer)

denied having authorised an executed payment – the payment service provider (in this case Starling) has to prove the payment transaction was authenticated. And if it is deemed that a payment transaction hasn't been consented to, it isn't authorised.

PSR 2017 goes onto say a payment service provider is required to refund the amount of an unauthorised transaction to the payer.

Mr S says he didn't consent to or authorise the payment to B and is seeking a refund of the payment made from his account. Starling says it considers the evidence suggests the payment was made by Mr S, and he is therefore liable for it. So, I need to think about whether the evidence I have suggests the payment was authenticated and whether it is more likely than not Mr S, or somebody with his knowledge or authority, carried out the payment Mr S is now disputing.

Having looked at all the evidence, which includes the technical evidence provided by Starling, I don't think it's unreasonable for Starling to have concluded that Mr S authorised the transaction. I say this because:

- From looking at the technical data provided by Starling, I can see that the disputed online payment from Mr S's account was made using Mr S's genuine card details.

- The payment was authenticated using Mr S's registered mobile device via Starling's mobile banking app. Logging into the online banking app requires customers to complete biometric security which customers create themselves when registering for online banking – in this case a PIN. So, I'm satisfied from Starling's technical evidence that Mr S's registered mobile device was used when the disputed payment was made, and that the transfers were authenticated as Mr S's correct security details had been entered to access the online banking app.

- The disputed transaction to B went through an additional layer of security to authenticate the payment. In this case, Starling has provided evidence that shows it sent an in-app message to Mr S's registered mobile phone to confirm the payment as genuine, which was approved.

- Mr S says he hasn't disclosed his online banking app security credentials to anyone. So, there's no reasonable explanation for how an unknown third party would be able become aware of these details to confirm the transaction.

.

- Mr S has said that around the time the disputed transaction was made he may have lost his mobile phone and replaced it with the same model. In other words, his usual phone wasn't used to approve the payment. But this is contrary to the technical evidence provided by Starling, which shows that no new devices were registered to access Mr S's online banking. And that Mr S's mobile device hasn't changed since September 2021. Therefore, there is no evidence of any other third-party device access or registrations.
- Mr S had approved other undisputed payments to different merchants before and after the disputed transaction (including on 10 June 2022). This indicates to me that Mr S was in possession of his device to make these payments as, while he claims his device was lost, he approved other payments using it, and carried out in app transactions including several faster payments.

- The IP address used to make the disputed transaction was one which had consistently been used for previous logins before the disputed transaction – and which continued to be used for logins after the disputed transaction to make undisputed transactions. In short, from looking at the technical evidence, I'm satisfied that the payment to B was authenticated from Mr S's mobile device, using his usual internet connection with his security and card details being required to access the online banking app and make the payment.

- Mr S has only disputed one transaction. It's more typical for the account to be used for as much as possible. But this didn't happen – only one transaction was made for a fraction of Mr S's account balance, which at the time had a balance of just over £10,000. Usually, a fraudster will try and maximise the usage of an account in order to get the greatest benefit from the account before the account holder notices their funds are missing and the card is cancelled. But this didn't happen.

- The disputed payment to B was made using Mr S's genuine bank card details being manually entered, including the CVV. Mr S said that he was still in possession of his card. Mr S's card details aren't visible when logging into his mobile banking app, which mean whoever made the transaction needed to be aware of these details or in physical possession of the card. There's no plausible explanation for how an unknown third party would gain access to Mr S's card details without his knowledge or consent. So, I can't reasonably conclude that an unknown party to Mr S made the transaction.

I recognise that Mr S has maintained that he didn't authorise the payment. But based on the evidence I've looked at it's hard for me to see how an unknown fraudulent third party could have obtained all of Mr S's security information, bank card, mobile phone and be in Mr S's normal location with all of these while making the payment. When I weigh everything up, on balance, the most likely explanation here is that Mr S made the disputed transaction himself. So, in the circumstances it wouldn't be fair for me to ask Starling to refund Mr S the disputed transaction.

In response to the investigator's view, Mr S has said that Starling should have refunded the disputed transaction when he reported it to them. But Starling has a right to investigate, and in this case determined Mr S wasn't entitled to a refund. So, I don't think it's unreasonable they didn't credit Mr S's account at the time.

Finally, Mr S has said that Starling has breached General Data Protection Regulation (GDPR) and the Equality Act 2010 because it didn't respond to Mr S's DSAR via the post. It's not the role or this service to say whether a business has acted unlawfully or not – that's a matter for the courts. It's also not the role of this service to decide whether or not a business has breached data protection laws – that's the role fo the Information Commissioner's Office (ICO). So, Mr S should raise his concerns directly with the ICO.

Our role is to decide what's fair and reasonable in all the circumstances. In order to decide that, however, we have to take a number of things into account including relevant law, which includes the Equality Act 2010, and what we consider to have been good industry practice at the time. And after looking at all the evidence, I've not seen anything to suggest that Starling treated Mr S unfairly when it said it couldn't respond to his DSAR by post.

In reaching this conclusion I recognise that Mr S had asked Starling for all communications to be sent to him by postal mail. However, Starling opted to send DSAR information via

email. Starling has explained that it does this due to the higher level of security that can be achieved over sending large amounts of secure data in the post. Given the sensistive nature of the informaiton that is usually contained in a DSAR response, I don't think this is unreasonable. So I can't say Starling has treated Mr S unfairly when it declined to send his DSAR information through the post.

My final decision

For the reasons I've explained, 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 S to accept or reject my decision before 21 August 2024.

Sharon Kerrison
Ombudsman