DRN-4248118

The complaint

E, a limited company, complains that Starling Bank Limited won't refund payments that it didn't make from its account.

What happened

The director of E says that his phone was stolen while he was using it at around 06:00 on 10 July 2022. He had been distracted by someone he'd been talking to asking for directions. Payments of a total of nearly £20,000 were made using the phone which weren't authorised. One only payment of just over £503 made using the card details was refunded. But four faster payments weren't.

Starling Bank said it wouldn't be refunding the other payments. It said that logging into the account would only be possible with a passcode as it understood that E hadn't set up biometric access. And setting up the new payee used here required a password. Starling Bank said E had agreed to the terms of conditions of the account which included keeping the security information and the device used to access the account safe. Starling Bank said that E was liable for the payments.

Our investigator didn't recommend that the complaint be upheld. He said that Starling Bank had shown that the password was correctly entered to make these payments. There was no identified way in which an unknown third party could have discovered this. The director said he hadn't disclosed this information or written it down anywhere. While the payments were large and confirmation of payee didn't show that the name on the payee's account matched the details given, this wasn't conclusive of someone else making the payments without E's authority. We provide informal dispute resolution and the director had told him that police were investigating the recipient's account based on what had been reported.

E didn't agree and wanted the complaint to be reviewed. The director said that he clearly didn't make these payments for E. And he had reported this to police and his phone provider. He wanted to know why Starling Bank had allowed this large amount of money to be sent to a new payee. He wasn't aware of who had received the money and there was no connection to E. This had caused significant financial problems for E, and he wanted answers from Starling Bank. He said it was nonsense that no refund was provided if he couldn't show how the password was discovered. This needed to be taken seriously.

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.

I need to take into account the Payment Services Regulations 2017 in considering this complaint. These state that a payment can only be authorised if it was consented to. So, it's not enough for it to be authenticated, say with security details. And if they weren't authorised E wouldn't generally be responsible for them.

There are exceptions to that and the relevant one here is whether the director acted with gross negligence in not keeping E's details safe. Negligence is often referred to as a failure to exercise reasonable care. So, I think it fair and reasonable to conclude, the use of 'gross negligence', rather than mere 'negligence', suggests a lack of care, that goes significantly beyond ordinary negligence.

So, I will be thinking about the following areas in looking at this complaint:
- What is the most likely explanation of how these payments were made?
- Did E either authorise the payments on the account or allow with gross negligence someone else to have access to the security information as Starling Bank says?

I won't be able to say *exactly* what happened and I'll be making findings about the relevant issues here based on what I think is *most likely*. It would be up to the authorities to undertake any criminal investigation.

A genuine device was used to access the account. This was one that E had used to make payments a few days earlier. I can see that a password was input to create the new payee at 06:38 on 10 July 2022 and then again to make the faster payments with the last one at 07:34. During this time the card payment referred to above using the mobile phone wallet was made at 06:54. I'm satisfied that these payments were authenticated.

I can see that the payments took all the available funds from the account. There were four faster payments of £5,000, £6,000, £8,400 and then £87.43. The card payment was eligible for chargeback and was refunded. There were no such rights for the faster payments. I note that the director said he noticed what happened on a second device at about 08:30. That's also consistent with Starling Bank showing that push notifications were sent for each payment, and it says these went to both registered devices. The director called Starling Bank at just after 14:00. There were no funds recoverable by that time. The device and card were then blocked.

To make the payments required access to the phone through any security set on that. Access to the app itself required a passcode. And to make the payments involved here required a password. The password had been set on the account in December 2021. And it hadn't been input for several days. So, there was no possibility of the director being seen say inputting the details before the phone was stolen that day. There is no record of either the password or passcode being changed before these payments.

I take into account the size of the payments, that these didn't have confirmation of payee (a match of the account name to the details given and which was overridden in the app) and that all the money was quickly taken. This has been reported to police and the chargeback was successful. And so, I can see why the director insists these are unauthorised payments that E isn't responsible for.

Against that I need to think about how the necessary security information could have been discovered by a third party. I'm afraid it's not enough to assert that it must have been. The director has said that it wasn't written down or stored anywhere and he hadn't told anyone. It was clearly used within a short period he says of his phone being stolen. I can't see it plausible to think that the information was guessed. Starling Bank says that as this was a company account such payments didn't trigger any concerns.

If I was to think that the security information had been disclosed or not kept safely then I'd consider here the director hadn't taken sufficient and reasonable care of the information and that this was gross negligence. This would be grounds for E being liable for unauthorised payments. I appreciate that this is how Starling Bank concluded that the details were

discovered. But the director has said he kept the details secure and on that basis there is no likely way in which an unknown third party discovered the details.

Having balanced all this information and what has been said on behalf of E I find it reasonable for Starling Bank to hold E responsible for these payments. I don't think it most likely that an unknown third party was able to discover the security information and make these payments if it had been kept secure as E claims happened. So, I don't find E's version of events to be reliable.

I appreciate what's at stake here for E and that it is continuing to pursue things with the authorities. But I don't have a reasonable basis to require Starling Bank to do anything further here.

My final decision

My decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask E to accept or reject my decision before 28 September 2023.

Michael Crewe
Ombudsman