

The complaint

Mr M has complained that Starling Bank Limited won't refund transactions he says he didn't make or otherwise authorise.

What happened

In late 2023, over £18,000 was spent on Mr M's Starling accounts over the course of about ten hours. The spending was mostly point of sale card payments, but also some payments made via his mobile phone.

Mr M says he'd gone to a house party and slept there. He says his wallet was taken with his cards inside, though his card with his other bank remained with him and he could not provide any evidence of replacing the other items in his wallet. His phone was not stolen, and was protected with a password and his biometrics. He didn't record his PIN nor tell it to anyone, and he hadn't set it to a number that could easily be guessed such as his birthday. He didn't record his banking security details anywhere nor share them with anyone either, all his passwords were different, and he had not engaged with any suspicious contact. He hadn't let anyone else use his account.

Starling held Mr M liable for the payments in dispute, as there didn't seem to be any likely or plausible way someone could've known his PIN, had access to his phone, and knew his banking security details, all without his consent.

Our Investigator looked into things independently and didn't uphold the complaint. Mr M didn't agree, so the complaint's been passed 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.

First, I understand that Mr M now wishes to dispute further payments which happened many months after the matter in dispute. But those happened well after this case came to our service, and Starling must have the chance to look into that matter first before we can. So if Mr M wants those payments looked at, he'll need to do so in a separate case to this one. Further, from what he's sent us, those payments were made at a very different time, to very different merchants, in a different continent to the payments I'm looking at under this case. So it's not likely that they bear any real relation to the payments I'm looking at here.

I also understand that Mr M would like us to investigate the merchants. But that is outside of our jurisdiction. We're not a police force, and we can only consider disputes about financial institutions – like Starling. Further, while Mr M pointed out that the merchants' addresses seem too far apart, it's not unusual for the address on the statement to be different from the place where the payment actually took place. For example, if the merchant lists its address as its head office, or uses a payment processor, and so on.

Turning to the matter at hand: broadly speaking, Starling can hold Mr M liable for the payments in dispute if the evidence suggests that he authorised them.

I'm satisfied from Starling's technical evidence that the payments in dispute used Mr M's genuine cards, and the correct PIN, as well as his genuine phone and app. So I can see that these transactions were properly authenticated. The question, then, is whether the evidence suggests that it's most likely Mr M consented to the transactions, or not.

To be clear, the genuine chips in Mr M's cards were read – these were not cloned cards. I don't have any evidence which substantiates that Mr M actually lost these cards – he says he lost his wallet, but he was unable to evidence replacing any of the other items in his wallet, and his card with his other bank remained in his possession. But even if I set that matter aside, the real crux of the issue is Mr M's PIN.

The correct PIN was used here – it was not bypassed. But Mr M said he didn't record the PIN anywhere or tell it to anyone. And he hadn't made any payments using his PIN in the recent time before this, so there was no reasonable opportunity for someone to watch him enter his PIN and then take the cards. His PIN was not a number which could plausibly be guessed, and it's exceptionally unlikely that a thief simply got lucky. This means there's no likely or plausible way that someone knew Mr M's PIN without his consent.

Similarly, Mr M's phone was used to facilitate the disputed payments. I'm satisfied from the technical data that this was Mr M's phone, from its the unique device ID, the model of phone, the IP address, and the fact that Mr M had registered it using a live video selfie. Mr M confirmed that he remained in possession of his phone, and I can see that's the case as he continued to use it for his mobile banking afterwards. There was no other active device registered to the account at the time.

There doesn't seem to be a likely or plausible way someone could've accessed Mr M's mobile app without his permission. The phone itself was protected by a unique passcode and Mr M's biometrics. There was a suggestion that someone could've scanned Mr M's face while he was asleep, but as standard Face ID requires one to have one's eyes open and be paying attention to the device, so it's unlikely someone accessed his phone that way. Then his mobile app was protected by further security details, which were not recorded anywhere or told to anyone. No malware was detected, and I've not found any signs of hacking. So there doesn't seem to be any likely or plausible way that someone could've accessed Mr M's phone and app without his permission. It's also notable that the IP address used for the disputed payments matches up to the IP address Mr M uses for his genuine activity.

While this is a more minor point, it's not very plausible that a thief would keep Mr M's wallet, but return his phone to him – despite having supposedly gained full access to it. This would be of no benefit to the thief – it would actively limit how much they could steal, while significantly increasing their chances of being caught while returning the phone. Similarly, I might have expected a thief to try to take as much money as possible as quickly as possible, before the account is blocked. But here, while the amount spent was significant, the person using the account left gaps of hours between attempting payments, didn't take any cash or spend as much as they actually could have, then stopped trying to make payments while there were still very substantial balances left in the accounts.

In summary, there's no likely or plausible way that someone knew Mr M's PIN and was able to access his phone and mobile banking without his permission. Whereas given that the payments were made with Mr M's genuine cards, PIN, phone, and mobile app, at his usual IP address, with his phone remaining in his possession, it seems both likely and plausible that the disputed payments could have been made with Mr M's consent – whether by himself or by someone he'd given his permission to. So I find it's most likely that the payments in dispute were authorised.

Mr M argued that Starling should've blocked the payments. I might have expected Starling to do that if they had good reason to think the payments were unauthorised, for example. But here, I've already found that the payments were most likely authorised. It follows that I can't fairly conclude that Starling needed to block them as unauthorised. Ultimately, they were made using Mr M's genuine cards, his correct PIN, and his genuine device, at his normal IP address, and he was sent notifications of the spending. And I don't agree that some payments being made in euros meant they had to be blocked.

I also understand that Mr M would have liked Starling to try a chargeback. But a chargeback is just another way to try to get a customer's money back. And while it's often good practice to try one, they are voluntary, and I'd only expect Starling to try one if it had a realistic prospect of success. Starling could have tried charging back these payments as being unauthorised. But again, I've found that they were most likely authorised. So it's not likely that such a chargeback would've succeeded, and Starling didn't have to try one here.

So based on everything I've seen, I find that Starling do not owe Mr M a refund for these payments. This is a difficult message for me to give, and I know it's a difficult message for Mr M to receive. But given the evidence I have, and the balance of probabilities, I'm unable to reasonably reach any other conclusion.

My final decision

For the reasons I've explained, I do not uphold this complaint.

This final decision marks the end of our service's consideration of the case.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 25 September 2024.

Adam Charles
Ombudsman