DRN-5812745

The complaint

A Ltd, represented by director Mr W, complained because Starling Bank Limited refused to refund transactions which Mr W said he hadn't authorised.

What happened

Overnight on 7th to 8th June 2025, Mr W was out with friends. He said he was trying to get a taxi when he was hit in the face. He said someone stole his phone and wallet. He immediately chased, and was helped by undercover police. The police arrested and charged the man. Mr W got his phone back. However, the police didn't find Mr W's wallet, containing his cards, on the man arrested.

Mr W froze his personal cards with a number of organisations, but he said he didn't think about his business account in the name of A Ltd until later that day. He then saw that there had been three debits just after midnight: two £200 card payments, and a £100 cash withdrawal. There had also been around 15 declined transactions after the ones which were paid. Mr W contacted Starling by chat, and said what had happened.

Starling cancelled Mr W's card, issued a replacement, and said it would investigate.

Later in June, Starling asked Mr W more questions. Mr W confirmed that he hadn't shared his PIN or written it down, and nor was it an obvious number. He told Starling that he was extremely careful with things like this. Starling also asked whether any of Mr W's cards with other organisations had been used, and he said he believed there had been an attempt but no money had been paid out.

Starling then told Mr W that it had concerns about the legitimacy of his claim, and it had concluded there hadn't been any fraudulent spend.

Mr W complained. He said there had clearly been fraud, clearly shown by 10 to 20 attempts to take money using various methods. He said that he had no idea how they'd managed to take the money, but it obviously wasn't him. He pointed out that he'd given Starling the police reference number which backed up that he'd been mugged and assaulted.

Starling sent Mr W its final response letter on 27 June. It said it had reviewed the previous investigation and communications, but it refused to change its decision. It also said that it wouldn't confirm any further details of its investigation.

Mr W wasn't satisfied and contacted this service. He set out what had happened, and said he was shocked that the thieves had managed to take money out without access to his PIN. But he said it was clear it had been a criminal act, because of various transactions coming out and being attempted; that he'd been with police at the times of some of the transactions; and the police had arrested someone for mugging him. He said he'd never given his PIN to anyone, even friends, and he'd never written it down. He said he hadn't used his PIN at any point that evening, and only uses the Apple wallet on his phone, almost never using physical cards. Mr W said he felt let down by Starling.

Mr W also provided information to evidence what he'd said. He sent us:

- a copy of a letter from a police witness care officer, which refers to Mr W being required to be a witness at a court case against a man accused of assault, theft and robbery;
- a screenshot showing that someone had tried to take £200 out of an account he had with a different bank, but he hadn't got this amount in the account at the time so it was rejected;
- a copy of his 9 June application for a replacement driving licence;
- copies of texts on 10 June, from two other banks, confirming that replacement cards had been requested.

Mr W said that he'd never made a claim like this before, either to Starling or any other bank accounts. He said it was the first time he'd been a victim of crime, and he'd previously thought he was very cyber aware and street smart, but was now even more careful when he was out.

Our investigator also obtained more information from Starling. This showed, as Mr W had said, that before the disputed payments there had been no genuine payments using the card's chip and PIN. Starling also told her that the reason why attempted payments after the three debits on 8 June had been declined was that the card had been locked. After that period, any further declined transactions were due to the card having been cancelled after Mr W reported it.

The investigator didn't uphold Mr W's complaint. She said that what she'd considered was whether the payments had been authorised by Mr W or not. As Mr W hadn't made any genuine chip and PIN transactions that day, there hadn't been any opportunity for a thief to ''shoulder-surf'' the PIN and find out what it was. Starling had also shown that the PIN hadn't been viewed on the app. As Mr W had said his PIN wasn't written down and he hadn't shared it, the investigator couldn't find a point of compromise. So she couldn't see how an unknown third party had correctly guessed Mr W's Starling PIN.

Mr W didn't agree. He said that of course he hadn't consented to the money being taken out. He said why would he go to the trouble of reporting to the police, locking and getting replacement cards, getting a replacement driving licence, and all the trouble of sending information to Starling and to this service. He said he'd never reported stolen funds before and this was a genuine complaint. He said that CCTV of the cash machine would show it wasn't Mr W making the transaction. He said that in his research, the only plausible thing he found was information about a card skimmer. He said he couldn't be the first person this had happened to, so he didn't understand why he couldn't be refunded. He also said that he'd never used his business account to spend money, and his transactions on the account showed he'd never taken money out of a cash machine with it. The account was strictly for business use.

Mr W asked for an ombudsman's 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.

I'm sorry to hear that Mr W was a victim of crime, which must have been very distressing.

What the Regulations say

There are regulations which govern disputed transactions. The relevant regulations here are the Payment Services Regulations 2017. In general terms, the bank is liable if the customer didn't authorise the payments, and the customer is liable if they did authorise them. So what decides the outcome here is whether it's more likely than not that Mr W, or a third party fraudster unknown to him, carried out the disputed transactions.

The regulations also say that account holders can still be liable for unauthorised payments under certain circumstances – for example if they've failed to keep their details secure to such an extent that it can be termed ''*gross negligence.''*

Who is most likely to have authorised the disputed transactions?

Mr W has submitted documentary evidence to back up his version of events that night. There's the police witness care letter, requiring Mr W to attend court as a witness in a case about assault, theft and robbery. There's also the evidence showing that there was a failed payment from an account which Mr W had with another financial organisation, and copies of texts showing that replacement cards had been requested from two other banks. There was also his request for a replacement driving licence.

The problem, however, is that the technical computer evidence shows that all three disputed transactions were carried out using Mr W's card and PIN. He said his card had been stolen, so it's understandable how that could have been obtained and used by a third party. But it's also necessary to know how Mr W's PIN could have been obtained by any third party.

Account holders have a responsibility to keep their PIN and other security details safe. Mr W was very clear that he hadn't told anyone his PIN, nor written it down. So this wasn't how any third party could have known the PIN.

Starling's computer evidence shows that Mr W's app hadn't been used to look up his PIN. The police found Mr W's phone, but not his wallet, in the possession of the man they chased and arrested, but there wouldn't have been time for the suspect to use the phone during the chase, which tallies with the computer evidence that the app wasn't accessed. So using the app wasn't how anyone obtained Mr W's PIN.

Similarly, there are no chip and PIN transactions in close proximity to the disputed ones. So no-one could have ''shoulder-surfed'' Mr W – in other words, watched him enter his PIN and memorised it. This ties in with what Mr W said about not withdrawing cash from his business account.

It's also most unlikely that anyone could have correctly guessed Mr W's four-digit PIN – because there are 10,000 possible combinations of a four-digit number.

Mr W suggested looking at CCTV from the machine where the cash withdrawal had been made. If CCTV was available at the machine where it was made, it would no longer be available, as it's typically only kept for around 30 days before being recorded over.

Mr W also suggested that a skimming device might have been the way in which a thief could have obtained his PIN. But skimming devices only take a sort of photo of the surface of the card and the information on it – and the PIN isn't recorded on the surface of a card. The chip is embedded within the card, and chip technology is complex and sophisticated. It's not generally thought technically possible to copy the chip on a card.

There was also, in Mr W's account of timescales, very little time between Mr W being mugged and the disputed transactions. This indicates that it's most likely that the person carrying out the disputed transactions already knew the PIN.

As I can't see how any third party fraudster was able to obtain Mr W's PIN, which was used with the card to carry out the disputed transactions, I have to conclude that it's most likely that Mr W authorised the disputed transactions. So Starling doesn't have to refund him.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask A Ltd, represented by Mr W, to accept or reject my decision before 12 December 2025.

Belinda Knight
Ombudsman