DRN-4723050

## The complaint

Mr B complains that Starling Bank Limited ("Starling") unfairly lodged a fraud marker against him.

## What happened

Mr B opened an account with Starling in December 2022. Later that month, the account received it's only incoming payment which was later found to be the result of a scam. The funds were sent to Mr B's account because the sender was fooled into thinking they were transferring funds for a legitimate reason. Those funds were quickly moved from the account by faster payments (bank transfers to other accounts) and cash withdrawals.

Mr B was asked about the activity on his account by Starling. They sent him several messages to obtain his explanation. Eventually he told them he'd been trying to get in touch about it and had also tried to freeze his card because he didn't recognise the payment. Mr B denied any knowledge of the incoming transfer and the outgoing payments. After reviewing the situation, Starling told Mr B they were closing his account. They also lodged a fraud marker with CIFAS – a fraud prevention service.

Mr B became aware of the marker when his current account (with another bank) was closed, and he had difficulty opening others. He approached Starling and asked them to remove it because he believed he'd been treated unfairly.

Starling didn't think they'd treated Mr B unfairly and declined to remove the marker. Mr B was left unhappy with their response and brought his complaint to the Financial Ombudsman Service for an independent review.

After an investigator was assigned to look into the complaint, Mr B gave his version of events which essentially said that he wasn't responsible for the movement of funds on his account and that a friend had used it without his permission.

Mr B gave various explanations about the account, including:

- He was asked to open it to make some easy money (which he refused to do).
- He was coerced into opening it.
- He was "blackmailed" into opening it.
- He opened it to save for university.
- He knew nothing about the scam payment or the outgoing payments.
- His friend had obtained all his passwords to use his account without his knowledge after taking his phone in the school library.
- His friend took his card and knew the personal identification number (PIN).

- His phone was hacked.
- He was tricked into giving his account details to "*someone".*
- The lack of an account has caused him difficulties and he was stressed and confused by the situation.

Starling provided details of their original investigation and exchanges they had with Mr B, in summary this said:

- The account only received one payment (the fraudulent one).
- Mr B set up the account and confirmed his identity with his passport and a selfie video.
- Mr B registered a second device with another selfie video.
- Mr B changed the password on the account.
- IP address evidence supports Starling's belief that Mr B was responsible.
- Mr B knew that Starling wanted an explanation about the payment, but he delayed getting in touch for about a week.
- There was no evidence Mr B had tried to get in touch earlier or freeze his card.
- Multiple passwords would have been required to access the account and set up a new payee – making it unlikely anyone but Mr B could have carried these out.
- Starling asked Mr B if he'd been asked to get involved with these transactions, but he denied any knowledge or responsibility.
- There's no evidence that Mr B reported his phone or card lost.

After reviewing the evidence, the investigator didn't think that Starling needed to do anything because they had met the necessary standards required to lodge a marker with CIFAS. It was also commented that Mr B's version of events was inconsistent.

Mr B disagreed and wanted to add that:

- Some of his evidence is no longer available.
- He's the victim and was used to commit a crime.
- His friend accessed the account from Mr B's device, but also hacked it.
- He was forced to hand over his phone.
- Mr B sent in messages from a friend supporting his version of events.
- He later admitted to opening the account, but his friend threatened to reveal information about him, which is why he gave him details about the account.
- He said the incident in the library happened during exam season ( March or May) but later (after he was told the dates of the account transactions) said this was probably

November or December.

The investigator considered Mr B's latest version of events but didn't change her opinion. As no agreement could be reached, the complaint has now been passed to me for a 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.

Starling, along with other banks monitor their accounts for suspicious activity. If they receive information about their account holder (as they did here), they're required to investigate the matter and report their account holder to CIFAS if certain standards are met. CIFAS are a fraud prevention service who maintain a register of persons linked to suspicious activity using their accounts. There are strict rules before lodging such a marker because having one in your name can cause difficulties obtaining financial products and they can last for up to six years.

There are two main parts to the evidence. One being that Starling had to have reasonable grounds to believe that a fraud or financial crime had been committed or attempted. Here they received notice from another bank that Mr B's account had received funds from a scam against the sending account holder. So, this gave Starling sufficient evidence to meet the first part.

The second part that Starling had to satisfy was that they must have clear, relevant and rigorous evidence that they could confidently report the matter to the police. That means it must be more than just a suspicion.

When they received the report from the other bank, they asked Mr B on several occasions to explain the payment and his relationship with the sender of the account. Mr B didn't respond for about a week despite evidence showing he was aware that Starling wanted to get in touch with him. He's also said he tried to get in touch and freeze his card because he was concerned at the time. I've not seen any evidence to support that, and Starling have no record of Mr B trying to get in touch with them. Given that all Mr B needed to do was to reply to the messages sent to him (which he did after about a week), I'm not persuaded by his story that he tried and failed to contact Starling at the time.

It's been difficult to unpick what Mr B has claimed happened because he's offered various versions of events depending on when and who he spoke with. He's variously said that he opened it to save money (at the time, Starling didn't offer a savings account) for university, he was coerced, he was blackmailed, and that he was offered easy money to open it. Mr B has also provided screenshots of a recent conversation with another friend discussing what happened in the library at school. Given the variety of stories presented by Mr B, I haven't put much weight on these screenshots.

What is apparent is that Mr B set up the account in mid-December (despite saying it was March/May) using his passport and various selfie pictures/videos. He then changed his password and added a new phone (again with his selfie), which took place on 23 December 2022. I would be surprised if Mr B was still in his school library, as he's stated, at that point in the year.

Activity with the phone continued the next day. The scammed funds landed in the account on 25 December 2022 ( Christmas day) at 11.35am. Records then show that the funds started leaving the account (cash withdrawals) at 11.49am and various bank transfers were made to other accounts. By early the next morning, the stolen funds were gone.

Mr B's phone and card were needed to make these payments. He's said it was his friend who had all the information after going through his phone in the library and taking his card. But the changes to the new phone and password were made when it was unlikely three friends were in a school library a few days before Christmas. Also, the IP address data shows the payments were made (on Christmas day) using Mr B's device from the same IP location that he'd earlier confirmed his ID with. It seems unlikely that his friend was responsible for this without Mr B's knowledge.

Note: IP addresses are a means to identify physical locations that online transactions/devices are connected to and can be their actual physical location or other locations connected to the provider of the data services.

Mr B has denied his involvement with payment into his account and the later transfers/cash withdrawals. I don't doubt there were others involved with this because that is generally how this type of arrangement works. But it seems unlikely that Mr B was unaware of what was happening at the time. I just don't think it's plausible that his phone was used without his permission, that his card was taken (and the PIN obtained), or that he was unaware of the arrangement. Whilst some of the money was sent to other accounts, a portion of it was taken as cash, so it's likely here that Mr B himself profited from the arrangement. When he was asked by Starling to explain what happened, Mr B denied knowing anything about it. If he's to be believed that he in fact did know something but was somehow coerced into it, then he missed an opportunity to explain that to Starling at the time.

I did consider Mr B's age at the time (17) when he opened the account and could understand if he was less than clear about what he was involved in. It's not unusual for younger persons to be co-opted into providing their banking details to others or fail to appreciate the implications of being involved in the movement of stolen funds.

Mr B is now a few years older and has since been given opportunity (in the current complaint) to re-examine those circumstances and his original involvement. If Mr B was caught up in the movement of funds innocently, then Starling could re-examine the marker. But, Mr B has continued to deny any involvement, despite the evidence showing the opposite of that.

So, I don't think that Mr B has given an accurate account of what happened because there are too many factors that show he was involved and knew what was going on. The account appears to have been set up solely to facilitate the movement of scammed funds – and the lack of any other payments into the account is evidence of this. The evidence also points to Mr B authorising those payments out of the account himself or enabling others to do so with his permission.

Overall, I think Starling met the standards laid down by CIFAS and it was both fair and reasonable to apply the marker against Mr B and I won't be asking them to remove it.

**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 Mr B to accept or reject my decision before 28 July 2024.

David Perry
**Ombudsman**