DRN-3731254

The complaint

Mr O complains that Starling Bank Limited added a marker to CIFAS, the national fraud database, when it closed his account.

What happened

Mr O says that someone stole his phone and was able to access his account at Starling Bank using the app. He says he has no knowledge of fraudulent payments into his account. The marker is affecting his ability to have an account at other financial businesses.

Starling Bank said it hadn't made a mistake and wouldn't be removing the marker. On 1 June 2022, payments of £3,500 and £1,432.18 were received into Mr O's account. It asked Mr O questions about the source of the money and wasn't satisfied with the response. Starling Bank received formal fraud reports. It didn't think that Mr O's account had been taken over as he says. Starling Bank said that the last device added to the online account was on 3 March 2022 which was verified with a video of Mr O. The password hadn't been reset since 5 May 2021. It closed his account and registered the marker.

Our adjudicator didn't recommend that the complaint be upheld. He explained that there is a high bar for adding a marker. Here there had been a report that fraudulent funds had been received. Mr O said that he'd lost his phone on 28 May 2022 while working late and couldn't find it. He'd said that the passcode on the phone and that on the app were the same. Mr O told him he wasn't sure if someone had hacked his phone.

Our adjudicator noted that Mr O hadn't reported his phone as lost until 6 June 2022 and he'd said the loss date was 3 June 2022, not 28 May 2022. This was after the funds had been received into his account. Starling Bank said it had sent the questions on Mr O's account to his email as well as on the app. There'd been no incorrect attempts to log into Mr O's account and no point of compromise for his details. And on 1 June 2022 a payee had been set up in Mr O's name for an account at a different financial business. It was unclear why this would have been done. And Mr O had confirmed he had other bank accounts including one at this other financial business. Our adjudicator said he thought it more likely that not that Mr O was complicit in what happened.

Mr O didn't agree and said he didn't see he'd been shown to be deliberately dishonest. He said when he spoke to the adjudicator he hadn't remembered the exact dates when he'd reported his phone lost: but the point was that he didn't have it at the time and wasn't aware of the payments. He said that anyone could send money to his account and he was *"helpless to stop them."* Mr O said he was certain that he hadn't received any emails with questions about the payments and that the first email was about the closure of his account. Mr O explained he'd recently been targeted by a hacker trying to get details of an account at a different financial business and he provided a video of screenshots showing this. He said that until this happened in September 2022 he had *"no clue that the last time it happened it was a hacker trying to access my starling account."* He said he believed and now remembered that this is *"exactly how the hacker gained access…"* He had no idea why a payee to his account at a different bank had been added but *"they had everything they needed to do that."*

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 won't be able to say *exactly* what happened and I'm thinking about what is *most likely*.

I need to consider whether the report to CIFAS was made fairly. On this point, Starling Bank needs to have more than a suspicion or concern. It has to show it had reasonable grounds to believe that a fraud or financial crime had been committed or attempted and that the evidence would support this being reported to the authorities.

What this means in practice is that a bank must first be able to show that fraudulent funds have entered the consumer's account, whether they are retained or pass through the account. Secondly, the bank will need to have strong evidence to show that the consumer was deliberately dishonest in receiving the fraudulent payment and knew it was, or might be, an illegitimate payment. This can include allowing someone else to use their account in order to receive an illegitimate payment. But a marker shouldn't be registered against someone who was unwitting; there should be enough evidence to show deliberate complicity.

To meet the standard of proof required to register a CIFAS marker, the bank must carry out checks of sufficient depth and retain records of these checks. This should include giving the account holder the opportunity to explain the activity on their account in order to understand their level of knowledge and intention.

I first can say that while I've seen the questions and answers about the payments, the evidence I have doesn't show that these were sent to Mr O's email account. I note that on 29 June 2022 when this issue had been put to him by Starling Bank he'd stated *"As I had lost my phone I didn't log in to my emails until the day when I called Starling upon reading my emails."* But then on 30 June 2022 that having checked his email *"The first email received was on the 13 June 2022."* I can't see that was formally challenged by Starling Bank with him.

I note what's been said about the loss of his phone. In his email of 27 June 2022 to Starling Bank Mr O stated he found he didn't have his phone on 28 May 2022. And that *"after a couple of days of not being able to find it I reported it to the police…"* The point is that he reported the loss date officially as 3 June 2022 and made the report on 6 June 2022. So that makes his supporting evidence about him not having his phone at the relevant time less helpful. I'd also expect a fraudster to act quickly on obtaining the phone as there'd be an immediate risk of detection and also of the phone and/or any apps being blocked, and it seemed to be at least three days before there was any use.

I note Mr O also refers in that email to an account being set up at a different bank using his details. The extract about this I've seen shows that a current account switching request had been set up from his Starling Bank account to that new bank account to complete on 23 June 2022. I consider that an odd thing for a fraudster to do.

I've looked at the issue of whether his account details were compromised. One possibility is that he was somehow shoulder surfed: but the last use of the account from his statement was in April 2022. And that also wouldn't explain how someone had worked out on what he says that his phone passcode and app passcode were the same. Another possibility is that his details were hacked. At the time of discussion about the compromise of his details with Starling Bank he said *"anything I say would be assumptions"*. I'm unclear when he says this specific hack of his details he now remembers happened. And in any event the nature of that

wouldn't explain how an unknown person involved also was able to obtain the device itself used to access the account and necessarily know the phone passcode even if the account details were somehow known.

Mr O says he's been in contact with the sender of the fraudulently obtained money who told him that his account was hacked to obtain money. The issue though is what happened to Mr O's account. He had no money in it before these payments. The purpose of a fraudster accessing it is unclear and so why the money would be sent to Mr O who says he's another victim. And there's also no real explanation from him about why attempts would be made to send the money on to another account in his name? Fraudsters will most likely access money as quickly as possible. And if a fraudster could set up a payee on Mr O's account it seems unlikely to be to another account of his even if that as Mr O says was possible. This all seems implausible to me.

Having considered all the evidence I find it *most likely* that Mr O was complicit in what happened and that he was either directly involved in the payments or that he allowed his account to be used by a third party in this way and for which he is equally responsible.

Starling Bank says that it applied the CIFAS marker because Mr O received fraudulent funds into his account. So, I've looked at whether Starling Bank was fair to apply the marker, based on the evidence it had, and the investigation it carried out. CIFAS guidance says the business must have carried out checks of sufficient depth to meet the standard of proof set by CIFAS. This essentially means that it needs to have enough information to make a formal report to the police. And that any filing should be for cases where there are reasonable grounds to believe fraud or financial crime has been committed, rather than mere suspicion.

Having reviewed Mr O's account of events and the evidence he has provided, I'm satisfied that Starling Bank had sufficient evidence for the CIFAS marker to be recorded. In coming to this view, I've taken into account the following reasons:

- Mr O received fraudulent funds into his account and didn't report this to Starling Bank at the time.
- He was in control of who had the benefit of this money.
- Starling Bank had grounds to believe that Mr O had been involved in the receipt and attempted dispersal of fraudulently obtained funds based on the evidence it had.

As a result, I also find there were grounds for it to decide to close his account. I appreciate what Mr O says about the impact of the marker for him. But I'm afraid I don't have a reasonable basis to require Starling Bank to do anything further.

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 Mr O to accept or reject my decision before 3 February 2023.

Michael Crewe
Ombudsman