DRN-3130615

The complaint

Mrs B has complained that Lloyds Bank PLC registered a marker against her at CIFAS, the national fraud database.

What happened

In August 2020, Mrs B opened a current account with Lloyds. She's confirmed that she received her card and PIN. She set up mobile banking on the same mobile phone number that she gave to our service, and it's recorded that she registered a fingerprint.

The account went unused until September 2020. Then over the course of a week, a series of substantial payments were made into Mrs B's account. The money was then either transferred out via an online cryptocurrency trading platform, or withdrawn at cash machines in Mrs B's local area using her card and PIN.

Later, several different people reported that Mrs B had received the proceeds of a scam.

Mrs B's testimony varied somewhat over the course of the case. At one stage, she said the account wasn't hers, but after the bank explained why they knew it was hers she accepted it was hers and explained she'd totally forgotten opening it. Mrs B said she was completely unaware of what had happened. She hadn't been checking her account because she'd been busy and there wasn't much money in it. At different points she said she'd opened this account either as a savings account, or to switch from her former bank, or to switch from a third bank.

Mrs B confirmed she'd received her card and PIN and registered the mobile banking app. She kept her card in her purse or a letter rack, and still had it after the fraud. She may have kept a record of her PIN. She didn't keep a record of her online banking details written down anywhere. She hadn't paid any money into the account. No one else had access to her account and she didn't know how it had been used. The only people who had access to her property were two close family members, her landlord, her cleaner, and her dog walker.

Lloyds closed Mrs B's account and registered a marker against her at CIFAS for misusing her facility and receiving wrongful credits.

Our investigator looked into things independently and didn't uphold the complaint. They couldn't see how someone could have made the payments involved without Mrs B's permission, not least given that her mobile phone, fingerprint, card, and PIN were used. It looked like Mrs B had been checking her online banking throughout and was aware of what was going on. And they noted that Mrs B's testimony had been contradictory in places.

Mrs B asked for an ombudsman to look at things afresh, so the complaint was passed to me to decide.

I sent Mrs B and Lloyds a provisional decision on 28 September 2021, to explain why I didn't think the complaint should be upheld. In that decision, I said:

In order to register this marker, Lloyds were not required to prove beyond all reasonable doubt that Mrs B had tried to do something wrong. They did need to have reasonable grounds to believe that she'd misused her account, which went beyond a suspicion or concern, and which had appropriate supporting evidence. I've carefully considered everything that both sides have said and provided. Based on what I've seen so far, I think Lloyds did have sufficient grounds to register this marker. I'll explain why.

First, I'm satisfied from Lloyds's technical evidence that the payments out of Mrs B's account used either her genuine mobile banking app, or her genuine physical card and the correct PIN. I'm also satisfied from the fraud reports that Mrs B's account received and passed on fraudulent money that had been taken from victims of scams. I've kept these facts in mind when thinking about what happened.

Mrs B says she got a message on social media from a man who'd been scammed by a young woman who had the same name as her. She didn't recognise the man or the young woman. I understand she hasn't kept a copy of those messages, so I can't see what was said. But from what she's told us, it was a very different scam from the one which her account was used for, so it does not appear to be relevant. But in any case, I've thought carefully about the possibility that an unknown fraudster could've used Mrs B's account.

The cash withdrawals in question were made using Mrs B's genuine card – and not a clone. It's technically possible that a thief could have stolen Mrs B's card, and she's said she may have kept a record of her PIN, too – so they might have learned her PIN that way. But Mrs B still had her card when she spoke to Lloyds after the fraud. So either it was never stolen, or it was given back to her. And I don't see any good reason why an unknown thief would go all to the effort of finding Mrs B again after the fraud and giving her card back. That would only increase the person's risk of being caught with no benefit to them.

Over the course of the fraud, Mrs B's mobile banking was used. But as I understand, Mrs B still has her phone. And her phone was used to make most of the transactions involved, at all hours of the day and over the course of a whole week. I think Mrs B would have noticed if her phone was missing for that long or if it was being repeatedly taken so often. And again, I can't see why a fraudster would go to all the effort and risk of giving her phone back after.

Mrs B didn't keep her login details written down anywhere and hadn't given anyone else access to her mobile banking. So there's no likely or plausible way that someone she didn't know could have learned those details and been able to log in without her consent. Further, her mobile banking activity was frequently verified using her fingerprint. And an unknown fraudster would not have been able to do that.

So I don't see a likely or plausible way that this fraud could have been done by someone who Mrs B's doesn't know.

It is possible that someone known to Mrs B may have made the transactions involved without her permission. But I don't think that's likely or plausible, either.

Understandably, Mrs B has effectively ruled out that her family members could have done this. And as I understand from her testimony, they had moved out of her home by this point anyway – so they would not have had the regular access to her property that was needed.

There were other people with access to Mrs B's property – her cleaner, dog walker, and her landlord. But as I understand, she never left them unattended. And these transactions were made over the course of a whole week at various times of day from the early morning to the late night – so those people would not have been able to access Mrs B's phone at such hours or with such frequency. It would also not have been possible for them to have been able to match Mrs B's fingerprint, and I can't see how they would've known her login details.

So I don't think it's likely or plausible that someone known to Mrs B did this, either.

Lastly, I've considered the possibility that Mrs B could have knowingly received the fraudulent funds, and either authorised the payments out of her account or let someone else use her account with her permission.

As I noted before, some of the activity involved was verified using Mrs B's fingerprint – which only she would have realistically been able to do.

The online payments were made using the same IP addresses that Mrs B had been checking her account from before the fraud. These IP addresses were located in Mrs B's local area under the internet supplier she uses. They appear to be Mrs B's IP addresses. And from what I've seen, only Mrs B knew the login details for her online banking.

The cash machine withdrawals were all made in cash machines near Mrs B's home, using her genuine card – which she still had in her possession afterwards – and the correct PIN.

Mrs B's account was not used for anything other than the fraud. As far as I can see, she opened the account, left it unused for a fair amount of time, and then it was used to receive and pass on money from the victims of crime. Mrs B doesn't seem to have tried to use the account for anything else. That doesn't particularly fit with this being a genuine account intended for genuine use. But it would fit with the possibility that Mrs B opened the account in order to help pass on fraudulent funds.

The fraud took place relatively slowly over a number of days, so the person using Mrs B's account does not appear to have been particularly worried that she would discover what was going on or stop them. This is only a minor point, but I might've expected a thief to try to use the account more quickly in order to lessen the risk of getting caught. More importantly, throughout the period Mrs B appears to have been frequently logging into her online banking – so it looks like she was aware of what was going on at the time and knew about how her account was being used.

There have been a number of inconsistencies in Mrs B's testimony. For example, she's told us and Lloyds different things at different times about why she opened the account and who had access to her property, and at one point she claimed it wasn't her account. Further, she said she never knew about these transactions and it wasn't her checking her account. But aside from the fact that her fingerprint was used to check her account at times, she also knew the balance of her account when she spoke to Lloyds afterwards – which she wouldn't have known if she hadn't been checking it. Indeed, if she hadn't known about the fraudulent credits and had never paid any money in herself, then I might have thought she'd have been rather surprised to learn there was any money in there at all. I do appreciate that Mrs B's told us she has problems remembering things sometimes. But this sort of contradictory testimony makes it very difficult for me to support her side of the story.

Finally, I've not seen any evidence that makes it seem implausible or unlikely that Mrs B could've authorised the account activity or given someone else permission to use her account.

In summary, I'm satisfied that Mrs B's account received fraudulent funds, and that her mobile banking, genuine card, and correct PIN were used to pass on the money. Based on the evidence, there isn't a likely way an unknown person did this, or that someone known to Mrs B did this without her permission. And given the times of the payments and the way they were authenticated, the only person who would reasonably have been able to get access to Mrs B's account so often was Mrs B herself. That leaves only one likely possibility – that Mrs B passed on the fraudulent funds or gave someone else permission to do so. And so I currently think that it was fair for Lloyds to close the account and register the appropriate marker with CIFAS. This is a difficult message for me to give, and I know it's a difficult message for Mrs B to receive. But given the evidence I have, and the balance of probabilities, I'm currently unable to reasonably reach any other conclusion.

I said I'd consider anything else anyone wanted to give me – so long as I received it by 26 October 2021. But neither Mrs B nor Lloyds sent me anything new to consider.

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.

Neither side have sent me any new evidence or arguments. So having reconsidered the case, I've come to the same conclusion as before – that the only likely possibility is that Mrs B passed on the fraudulent funds or gave someone else permission to do so. And so I think that it was fair for Lloyds to close the account and register the appropriate marker with CIFAS. This is a difficult message for me to give, and I know it's a difficult message for Mrs B to receive. But given the evidence at hand, and the balance of probabilities, I'm unable to reasonably reach any other conclusion.

My final decision

I don't uphold Mrs B's complaint in this case.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs B to accept or reject my decision before 24 November 2021.

Adam Charles
Ombudsman