DRN-4209368

The complaint

Miss R has complained that Monzo Bank Ltd registered a marker against her at CIFAS, the national fraud database.

What happened

Both sides are most familiar with the case, so I'll summarise what happened in brief.

In March 2021, Miss R's Monzo account received a credit of £9,800. Miss R's Monzo app was used to forward this money on quickly in two bank transfers. Monzo later found out that the credit was the proceeds of fraud.

Monzo closed Miss R's account and registered a marker against her at CIFAS.

Miss R has explained that, in June 2020, a thief robbed her of her phone. She'd left her phone unlocked and unprotected, and she'd recorded all her security details on it in an undisguised format, so she suggested the thief gained access to her account that way. She didn't tell Monzo about her phone at the time due to her mental health, and because the terms and conditions said she only had to report her card as missing. She also lost her card, but didn't report that missing either, because she used Apple Pay instead. She was adamant that the fraudulent credit and the subsequent outward payments happened without her knowledge or consent, and she didn't authorise them. She hadn't noticed anything was wrong at the time as she wasn't looking at her account and had turned notifications off.

Our investigator looked into things independently and didn't uphold the complaint. Miss R appealed, so the complaint's been passed to me to decide.

I sent Miss R and Monzo a provisional decision on 22 June 2023, to explain why I didn't think the complaint should be upheld. In that decision, I said:

First, I will clarify that while I have considered everything both sides have submitted, we are an informal alternative to the courts, and we don't look at things in quite as formal a way as the courts do. So I won't address the case on a point by point basis. Instead, I will focus on what I have found to be the key points.

In order to register this marker, Monzo were not required to prove beyond all reasonable doubt that Miss R had done 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. Having carefully considered everything that both sides have said and provided, I currently think that this marker does have sufficient grounds. I'll explain why.

I'm satisfied from Monzo's technical evidence that the payments in dispute used Miss R's mobile app and security details, on her registered mobile phone. I can see that these transactions were properly authenticated. The question, then, is whether they were made with Miss R's consent or not.

First I've considered the possibility that this was done by someone who Miss R didn't know – for example, a third-party thief.

The phone used to forward on the fraudulent funds was not the phone which was stolen in June 2020. The phone which was stolen in June 2020 was never used to access Miss R's Monzo app afterwards.

The phone used to forward on the fraudulent funds was one Miss R registered after her previous phone was stolen. It was the only device active on the account in 2021, and was the same device Miss R used for her genuine account activity both before and after the fraud incident. I am satisfied that this was Miss R's current phone at the time.

The fraudulent funds were forwarded on at the same IP address Miss R used frequently for her genuine account usage both before and after the fraud incident. This indicates that it was done in a location where Miss R usually carried out her online banking, such as her home.

The fraudulent funds were sent on to a payee I'll refer to as D. D was set up as a payee on Miss R's account not in March 2021, but in February 2021. Miss R's phone was used to send D £1,500 on 17 February 2021. Again, this was done at an IP address which Miss R frequently used for her genuine activity. This £1,500 payment was made using almost all of Miss R's account balance at the time. Miss R accessed her online banking very often after this payment and made other, genuine payments from the same device at the same IP address in the days afterwards. But she never reported that £1,500 as unauthorised or unusual, even though it used up nearly all the balance. This strongly suggests that the payment to D in February 2021 was genuine.

So the stolen phone from 2020 was not relevant to the fraud. In 2021, it was only Miss R's genuine, current phone which was used, from the usual locations where she carried out her online banking, accessed in the usual way. From the evidence, there does not appear to have been any unauthorised access to her account even after her old phone was lost.

According to statements Miss R's representative took, Miss R immediately told a family member – a police officer – about her stolen phone back in 2020. They helped Miss R wipe her old phone, and gave her advice on cyber-security, such that she became extremely aware and fully enlightened about phone security. Meanwhile, Miss R said she always had her phone with her. And I can see that her 2021 phone was not stolen, as she was still using it to access her account and correspond with Monzo after the fraud incident.

Putting all that together, I do not see a likely or plausible way that a third-party thief could've gained possession of Miss R's 2021 phone, accessed it without her consent, and given it back to her, all without her noticing, and all at the usual locations where she carried out her normal online banking – on at least two separate occasions in different months. Indeed, it is not plausible that a thief would give Miss R's phone back to her at all after stealing it – that would substantially increase their chances of being caught while actively reducing how much they could benefit from the theft.

Further, I'd expect a thief to try to use the account as much as possible, as quickly as possible, before the fraud is found out and/or before the account is secured. It is not likely or plausible that they would wait eight months to access Miss R's account after stealing her phone with her details on it, then wait a further month to use it again.

While Miss R says she wasn't checking her Monzo account, I can see that she actually used the account frequently and accessed her online banking quite a lot after the payments to D in both February and March 2021. I am satisfied this was her as she accessed her account to carry out other genuine, undisputed activity. And the February payment to D used up nearly all of her account balance. But again, Miss R didn't tell Monzo anything was wrong at the time. It is most likely that Miss R was aware of these payments at the time, and it is very unlikely that she would not report the payments if they were made without her consent.

Taking everything into account, it is not likely or plausible that an unknown thief did this.

It is technically possible that someone close to Miss R, such as a friend or family member, may have made the payments to D without her permission. But I find that that is not likely or plausible either.

Miss R's previous phone, with her security details on it, was stolen by an unknown third-party – not by someone she knew. So the stolen phone wouldn't be relevant. And Miss R confirmed that she didn't give anyone else access to her account, nor keep a record of her security details after that incident. So there's not a likely explanation for how a known party would've learned Miss R's security details in 2021. It's not clear how they'd be able to get through the 2021 phone's lock, either. Again, it's not very likely that they could take the phone, use it in Miss R's usual locations, and replace it, at least twice in different months, all without Miss R ever noticing, despite her keeping her phone with her. And this possibility doesn't explain why Miss R chose not to report any of the payments to D as unauthorised when it looks like she would've been aware of them at the time or shortly afterwards.

I find that it's not likely or plausible that a known party did this without Miss R's consent.

I've then considered the remaining possibility: that Miss R either forwarded on the fraudulent funds herself or gave someone else permission to do it for her.

This possibility is very well supported by the circumstances of the case and the evidence at hand. It neatly explains how someone had access to Miss R's 2021 phone – the only active device on the account, how they accessed it from her usual IP addresses, how they knew her security details, why Miss R didn't report the payments to D as unauthorised when she would've been aware of them, and so on.

I note that while Miss R claims her card was also stolen, she not only never reported it as lost or stolen, but continued to use it for her genuine spending. I can see that the genuine chip in Miss R's physical card was read a number of times for Miss R's usual spending right through to March 2021 inclusive. There was only one card on the account. I'm satisfied that Miss R's card was not stolen. This is only a more minor point, but it also calls Miss R's testimony into question. As I've explored above, the evidence also contradicts her testimony about which phone was used and about her not checking her account.

I've not seen any evidence which shows it's implausible or unlikely that Miss R could've authorised these payments or given someone else permission to make them. Ultimately, this is the only likely or plausible possibility at hand.

In summary, I'm satisfied that Miss R's phone and app were used to forward on fraudulent funds, to a payee which Miss R appears to have set up and paid previously, at IP addresses that match with her genuine use. I'm satisfied that the phone in question was not lost, as Miss R continued to use it afterwards. It is not likely or plausible that this was done without Miss R's knowledge or consent, either by an unknown or known party. The only likely and plausible possibility remaining is that Miss R forwarded on the fraudulent funds or gave someone else permission to do it. Miss R has not provided any evidence that she was entitled to the money, and confirmed that she cannot evidence any entitlement.

So it seems fair that Monzo keep the appropriate marker registered at CIFAS. It also seems fair that they closed Miss R's account, which they were allowed to do under the terms. CIFAS markers last for six years, and I have found no good reason why this one should be removed. This is a difficult message for me to give, and I know it's a difficult message for Miss R to receive. But given the evidence I have, and the balance of probabilities, I'm currently unable to reasonably reach any other conclusion.

Lastly, Miss R's representative suggested Monzo should've blocked the payments which forwarded on the fraudulent funds. But I'm afraid that's not relevant to this case. Even if Monzo had blocked the payments, they would still have been entitled to register and maintain a CIFAS marker against Miss R for attempting to forward on fraudulent funds – regardless of whether she was successful in doing so or not.

I said I'd consider anything else anyone wanted to give me – so long as I received it before 20 July 2023. Monzo accepted the provisional decision and confirmed they had nothing further to add. Miss R and her representatives didn't respond.

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, and for the same reasons as set out in my provisional decision above.

My final decision

I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss R to accept or reject my decision before 21 August 2023.

Adam Charles
Ombudsman