DRN-5927059

The complaint

Miss V complains Monzo Bank Ltd recorded a marker against her on a fraud database. She doesn't think it's treated her fairly.

She brings this complaint with the help of a representative; however, I will mostly refer to Miss V in my decision because she held the relevant relationship with the bank.

What happened

A summary of events is below.

Miss V held an account with Monzo which received £670 through a bank transfer in April 2025. £500 of this was transferred to an account she held elsewhere (Revolut). After this, £489 of the funds were sent to Western Union. However, the original incoming payment was later reported to Monzo by another bank as being the result of a fraud.

Monzo restricted the account and requested information to support why Miss V had been entitled to the funds. When it didn't get a response, it filed a misuse of facility marker at Cifas, as it believed she had been complicit in receiving and benefitting from fraudulent funds. It also closed the account. Miss V found out about the marker and complained that she'd not done anything to cause this. She asked Monzo to remove the fraud marker.

Monzo reviewed the loading, but it didn't think it had made a mistake. Dissatisfied, Miss V contacted us and said the marker was affecting her financially and personally and she wished to challenge the bank's decision.

One of our investigators reviewed the case and gathered some information. Miss V told the investigator that her iPhone had been lost/stolen on 23 March 2025, whilst out in London and as soon as she'd arrived at her sister's, she'd logged into her device and activated the Lost Mode for it. Also, as she needed a functioning device, she purchased a replacement phone the next day, which an Apple employee synched using her iCloud settings. Subsequently, she started to receive notifications that her Apple ID had been used on a Windows device she did not recognise. She said that she contacted Apple customer services to report this, who advised her to change her password, which she did. However, she got another notification that her old iPhone had been located overseas.

Miss V said that she hadn't realised anything untoward had gone on with her Monzo and Revolut accounts until now and believed whoever had taken her iPhone was responsible, stressing that none of this had anything to do with her. The investigator asked Miss V some further questions about how she usually accessed her phone, accounts and the app, together with how her security credentials were stored. However, after weighing this, and the other evidence, he felt Monzo had enough information to support its decision to load her onto Cifas. He noted several concerns but especially that Miss V had said her iPhone needed PIN/face ID to get into it, and she'd also said she didn't have her account log in details stored on the phone. So, he couldn't see how a fraudster could have got into her phone to carry out the activity without her involvement. He also shared Monzo's

apprehensions about the movement of the funds and overall activity submitting this wasn't typical of a fraudster.

Miss V disagreed with the outcome and made some further representations, including through her solicitor. Amongst other things, she said she'd been mistaken when she'd said she hadn't stored her account log in details, she'd since remembered they were in a document accessible in the Notes app, and that it was believed she must have been shoulder surfed for her phone PIN. She also referred to the notifications she'd had from Apple which she felt were demonstrative of third-party involvement and added that she'd never paid close attention to her Monzo and Revolut accounts as neither of them were her main bank account (providing statements), and thus she hadn't seen the funds come in and move as they did. Neither had she seen Monzo in app notifications.

She accepted she'd been remiss in not reporting the loss of her phone to Monzo in order to secure her account but didn't think this had meant she was complicit in fraudulent activity. She also referred to the police reports she made and her engagement with Western Union about the transaction there and felt our service ought to look into that further.

The investigator issued further assessments, setting out his analysis as to why he still believed the available evidence suggested Miss V had been complicit in receiving and benefitting from fraudulent funds. He was satisfied Monzo had met the threshold for loading the marker. Monzo also reviewed the investigator's assessments and Miss V's further documents and submitted that the loading should remain, as it continued to hold concerns about the account activity, believing Miss V had access to her account and app at the relevant time. Overall, it believed there was enough to show Miss V was complicit in what had happened.

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 satisfied I have enough information to determine this complaint.

The marker that Monzo has filed is intended to record that there's been a 'misuse of facility'– relating to using the account to receive fraudulent funds. To file such a marker, it's not required to prove beyond reasonable doubt that Miss V is guilty of a fraud or financial crime, but it must show that there are grounds for more than mere suspicion or concern. The relevant guidance says, there must be reasonable grounds to believe that an identified fraud or financial crime has been committed or attempted, and the evidence must be clear, relevant, and rigorous.

What this means in practice is that the business must first be able to show that fraudulent funds have entered Miss V's account, whether they are retained or pass through the account. Secondly, the business will need to have strong evidence to show that Miss V 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 to receive an illegitimate payment. But a marker should not be registered against someone who was unwitting; there should be enough evidence to show complicity.

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

So, I need to decide whether I think Monzo has enough evidence to show fraudulent funds entered Miss V's account and she was complicit. And I'm satisfied that it has. I'll explain why by addressing what I consider are the material points.

Monzo has provided evidence that it received a report, saying that funds which entered Miss V's account was because of a fraud. I've examined the report, and I'm satisfied the bank had reasonable evidence of a fraud and needed to make enquiries to meet its regulatory obligations to investigate such matters. I'd like to assure Miss V that I have reviewed this evidence impartially and objectively as my role requires.

Monzo contacted Miss V in her app and by email for her to contact it and explain why she'd received the payment, so I'm satisfied that she was given a fair opportunity to explain her side of things. She says she didn't access the app after her phone was stolen because Monzo wasn't her main bank account, but the available evidence doesn't support what she's said. I've reviewed in-app chats from early April. Miss V contacted Monzo to say that she had received a notification about her new card, which she also verbally told the investigator about when he was gathering information. So, if Miss V had access to it, then her testimony about not going into the app (she said the last time was March 2025) isn't credible. Also, as well as the in-app notifications, Miss V was sent an email from Monzo saying that the bank was trying to reach her. Even if this wasn't her main account and she was busy, it's not enough to explain why she didn't pursue contact with the bank as Monzo was telling her that it was trying to reach her.

After not hearing from her, Monzo decided to record the fraud marker. I don't think that was unreasonable given the above. It also decided to retain the marker, after reviewing the case following Miss V's complaint and further information. I've looked at what Monzo has, and I don't find its position unjustified. First, whilst shoulder surfing for the phone PIN has been asserted, there isn't any specific evidence to support that's what happened here.

Miss V has also changed her testimony; after confirming she didn't have her bank passwords stored. She now says, she later realised these were included in a single file and accessible on her old phone. On this point, I've looked at the file she's provided, and I can see she's been meticulous at keeping her PINs, codes and passwords in the document. She's also said that she went into her iPad on 23 March to delete the password file from it,

"*On 23 March evening, while attempting to secure my information after losing the phone, I deleted the file from Notes on my iPad and moved it to the Files app. Unfortunately, as both my iPad and iPhone are linked to the same iCloud account, this action also made the document accessible on the lost phone*."

If I'm to believe Miss V was concerned about the information (in the file document) being accessible after losing her phone, I think it's odd that she wouldn't remember what was in it. Thinking about the points together, I'm not persuaded that she was mistaken when she initially said she didn't have a note of her banking credentials and so I don't find her testimony reliable.

Beyond this, there is also the account activity where an alleged fraudster left £170 in her Monzo account. I have read Miss V's solicitor's comments about layering etc, but this was a single incoming transaction into her Monzo account. I think it's more likely for a fraudster to want to get hold of the funds before the sending bank reported the fraud and it's less likely for a fraudster to be concerned about leaving some money in the account to avoid detection. In addition to this, I don't see why the funds would need to go to another one of Miss V's accounts when the fraudster could send the funds anywhere. The account activity when looked at everything else that Monzo has doesn't stack up.

As part of my role, I must look at what both sides have provided and consider the weight of the evidence. Here, although Miss V has attempted to explain things (particularly highlighting the messages from Apple) and provided supporting information, I have to say whether I think Monzo has enough to justify its actions in making the filing to Cifas and continuing to maintain it. Overall, I'm satisfied Monzo has sufficient information to support its actions that it believed Miss V had been complicit in receiving illegitimate funds, with the report it received, her not responding to its attempts to contact her and get information about the payment, her recollections about her storing her account details and the activity with the funds.

It follows that I don't find recording the marker and closing the account was unfair (for completeness there's provision for that in the account agreement).

I understand Miss V feels strongly about her complaint and the affect the marker is having on her, but I must also look at the evidence objectively and these are my conclusions based on the available evidence. Whilst my decision ends our review of her complaint, there's nothing preventing Ms V from pursuing it through alternative means, for example, the courts.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss V to accept or reject my decision before 11 February 2026.

Sarita Taylor
Ombudsman