DRN-5085330

The complaint

Miss B complained because Metro Bank PLC refused to refund her for transactions which she said she hadn't authorised, and then closed her account.

What happened

On 17 May 2024, Miss B contacted Metro. She said there had been transactions on her account which she hadn't authorised. The transactions were:

- Four card payments totalling £172.47, between 27 and 29 April. Two of these were made by mobile payment service, and two were online card payments; and
- Three internet banking faster payments totalling £1,222, between 26 and 29 April.

Metro replied that the disputed payments had been made after the correct security information had been provided. And the mobile device used to make the payments had been registered to Miss B's account since 31 October 2023, and it had also been used for undisputed payments. Metro also pointed out that before a new payee was set up, a one-time passcode (OTP) had been sent to the registered mobile.

Metro asked Mis B for more information. It asked her whether she'd received any unusual calls, texts, or anything else unusual, and asked for screenshots of any of these. It also asked what information she'd handed over, if she had, and if she'd bought any goods, where she'd bought them from. In reply on 10 June, Miss B sent a screenshot of her Metro app, which wasn't relevant to the case.

On 12 July, Metro rejected Mis B's claim. It said that it had sent an online banking authorisation request to her about the setting up of the new online payee. Metro's authorisation message had said *''Is it you making this transaction online? Only chooses 'continue'' if you want to authorise this online card transaction. If someone has told you to approve this transaction it could be a scam. If you confirm this transaction and it turns out to be a scam, it is unlikely that you will get your money back.''* It had received a response back confirming it was genuine.

And Metro also said that for the mobile payment service disputed payments, it had sent her a text authorisation code, which again had been completed successfully. It pointed out that to authorise this type of payment, Miss B had had to use fingerprint or face ID, or input her device password.

So Metro said that this meant it was reasonable to assume that Miss B had authorised the disputed transactions herself, or hadn't taken adequate care of her security details. This meant it wouldn't refund her. It pointed out that false claims of fraud could be registered with other financial organisations and fraud prevention agencies.

On 12 July, Metro decided to close Miss B's account. It wrote to tell her the account would be closed on 19 July, so she had to withdraw her funds, settle any outstanding payments, and tell anyone who sent her payments to the account. It said it wouldn't offer her any new banking services in future. Metro referred Miss B to section 11.2 of its service relationship document.

Miss B complained.

Metro issued its final response on 18 July. In relation to the closure, it said the decision to close Miss B's account hadn't been taken lightly, and was in line with term 11.2 of its service relationship document. In relation to the disputed payments, it said that the recipient retailer had provided more information which confirmed the details it had for Miss B, which matched what Metro had for Miss B's name, address, and IP address (a unique computer identifier). Metro also repeated that it had sent an authorisation request to Miss B's online banking, and had had a confirmation back from her. It also repeated that the mobile payment service payments had been authorised following a text to Miss B's registered phone, which had been used for undisputed payments. And to authorise a mobile payment service payment, Miss B would have needed to use her fingerprint/facial recognition, or her phone's passcode.

So Metro refused to refund her, or to keep her account open.

Miss B wasn't satisfied and contacted this service.

Our investigator asked Miss B for more information. This included asking whether Miss B had lost her mobile around that time; whether anyone else had access to it; whether it was password protected; whether she'd clicked on any links or downloaded any software; when she'd noticed the disputed transactions; and whether she'd reported the fraud to the Police or Action Fraud.

Miss B didn't reply.

Our investigator didn't uphold Miss B's complaint. He said that:

- the mobile payment transactions had been completed using a token that had also been used for genuine transactions. Miss B hadn't reported her phone compromised or lost, so it was likely that she'd authorised them;
- the other card transactions had been online, completed using 3D Secure (3DS). The device used had been used by Miss B before and after the disputed transactions, and she hadn't mentioned any compromise to the device. So only Miss B could have authorised the transactions;
- the online faster payments had been made to a beneficiary set up on 26 April to a beneficiary set up using a OTP to Miss B's mobile. This device had been used before and since for undisputed payments;
- when Metro sent us its submissions for Miss B's case, it said that it believed it had been right to close Miss B's account, but should have given her 60 days' rather than 7 days, and said it offered her £100 compensation. The investigator said this was fair.

Miss B didn't agree. She said that on 29 April she'd had a text asking her if she recognised a payment for £711.33, which had been declined. She said this was how she found out about the transactions. She said she'd asked Metro about the type of phone used for the disputed transactions, and it was a different one from hers.

Miss B also sent a copy of an email she'd sent to Metro in June. This said she'd never received any messages or authorisation requests for the disputed payments. She said she didn't understand why Metro was saying she'd authorised the payments, as it wasn't the first year she'd had a Metro account. She said that Metro saying she'd authorised the transactions was defamation and intimidation. She said she just wanted her money back and Metro should be doing its job and protecting her money.

Miss B asked for an ombudsman's 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.

What the Regulations say

There are regulations which govern disputed transactions. The relevant regulations here are the Payment Services Regulations 2017. In general terms, the bank is liable if the customer didn't authorise the payments, and the customer is liable if they did authorise them. The regulations also say that account holders can still be liable for unauthorised payments under certain circumstances – for example if they've failed to keep their details secure to such an extent that it can be termed ''*gross negligence.''*

So I've looked at the evidence to decide whether it's more likely than not that Miss B, or a third party fraudster, authorised the disputed transactions.

Who is most likely to have authorised the disputed transactions?

Metro provided technical computer evidence. This shows, among other things, that:

- the two mobile payment transactions were authorised using a token which had also been used for genuine transactions on Miss B's account;
- Miss B hadn't previously reported her registered device lost or stolen, either to Metro or to the police;
- the online card transactions were carried out using 3DS, which requires an extra level of security. Whoever authorised the card transactions had access to Miss B's device which she used for undisputed transactions before and after the disputed ones;
- the faster payments were made to a beneficiary that was set up on 26 April, with a OTP sent to Miss B's registered mobile to approve the setting up of the new beneficiary. Miss B said she never received any alerts but I've seen the computer evidence that it was sent to her registered mobile, and approved.
- the device used to access online banking and carry out the faster payments on 26 and 29 April was the same device which Miss B had used before and after that, for undisputed payments.

I find the technical computer evidence compelling. And Miss B didn't respond to our investigator's questions to give her side of the story. So I find that it's most likely that Miss B authorised the disputed transactions herself.

Looking at the objections sent by Miss B after our investigator issued his view, I find it surprising that Miss B said she'd had a text about a payment which had been declined on 29 April, but hadn't received any of the texts about earlier payments. I think this is unlikely, as all Metro's messages were sent to the same phone which was already registered to her Metro account.

I note that Miss B said she didn't understand why Metro was saying she'd authorised the payments, as it wasn't the first year she'd had a Metro account. But how long she'd had a Metro account makes no difference to Metro's assessment, or to my decision, about whether or not it's likely that Miss B authorised the payments herself. I note that Miss B said Metro had defamed and intimidated her, but I don't agree with this. I find that Metro took its decision on the technical evidence it had, which indicated that it was more likely than not that Miss B authorised the payments herself.

Metro's closure of Miss B's account

Metro's Service Relationship document contains the terms and conditions of Miss B's account. Section 11.2 sets out, among other things the circumstances in which Metro could stop providing banking services. There are many possible situations set out in this section. Having considered these, I find that Metro didn't act unfairly when it closed Miss B's account in all the circumstances here.

I have also considered the notice Metro gave Miss B. Section 11.2 says about account closures:
''We may do this immediately…
If we suspend a service or close an account, we will take reasonable steps to reduce the inconvenience to you. If we can, we will tell you before we suspend the service or close the account (usually giving you two months' notice).''
So this gives Metro the power to close an account immediately, or with two months' notice. I note that Metro initially gave Miss B 7 days' notice, which is neither of these, but it has recently decided that it should have given her 60 days' notice and therefore offered £100 compensation. I leave it up to Miss B to decide whether she wishes to contact Metro to accept that offer.

My final decision

My final decision is that I do not uphold this complaint. I leave it to Miss B to decide whether or not she wishes to contact Metro to accept its offer of £100 compensation for giving her 7 days' notice of closing her account, rather than 60 days' notice.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms B to accept or reject my decision before 27 January 2025.

Belinda Knight
Ombudsman