DRN-6196257

The complaint

Miss H complains that Modulr FS Limited hasn't reimbursed two payments she says were unauthorised.

Miss H has an electronic money account with Pockit, which is provided by Modulr FS Limited. As the transactions being complained about were faster payments from Miss H's Pockit account, Modulr is the correct respondent business here. But as Miss H's communication was with Pockit, for ease of reading, I'll refer to Pockit throughout my decision.

What happened

Miss H is disputing two payments of £520 and £480 on 2 May 2025 which she says she didn't make. The Pockit account was opened on 27 April, with the first transaction – a credit for around £1,140 – being on 2 May. Miss H says when she logged on to check if the funds had come in, she also noticed the two payments in question. She transferred the remaining funds and changed her account password.

At the time of reporting the matter to Pockit, Miss H said her account had been hacked. She said she didn't share her account security details with anyone.

Pockit declined to reimburse Miss H on the basis that the security information sent to her registered contact details would have been required for the transactions to take place. It said it couldn't conclusively determine that this information was compromised without Miss H's involvement.

Unhappy with this outcome, Miss H referred the matter to our Service. She said she was unhappy Pockit didn't alert her about the transactions, and this prevented her from being able to stop them leaving her account. Miss H mentioned that her wallet, her phone and her passport were lost in a public place prior to the disputed transactions, and she thought this may have allowed the fraudster to gain access to her personal information. Miss H also mentioned that her iCloud account had been hacked a few months prior.

Our Investigator didn't uphold the complaint. They said there were several discrepancies in Miss H's recollection of events, and they weren't persuaded that the payments were unauthorised.

Miss H didn't agree. In summary, she said she'd provided enough evidence and information to show that a third party had accessed her account. The Investigator considered Miss H's comments, but they weren't persuaded that a third party was able to register a new device – which was used to make the disputed payments – using information that was sent to her email address and phone number without her knowledge.

As the matter couldn't be resolved informally, the complaint was referred for an Ombudsman's review. After the complaint was passed to me, I contacted Miss H and said I'd noted that in one of her emails to Pockit she'd said the fraudster had approached her regarding a work from home job and she sent the two amounts in question to purchase

equipment. She'd also said she didn't hear back from the individual after the payments were made. I asked Miss H about this and sought clarification on what happened at the time which led to the payments.

Miss H asked me to disregard the information about the home job and said she was pursuing other complaints involving a different bank at the time of the email in question, and she got the details mixed up. She reiterated that she didn't make or authorise the disputed payments, and the evidence provided showed unauthorised access by a third party.

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.

Having done so, I'm not upholding this complaint for similar reasons given by the Investigator. I know Miss H will be disappointed with this outcome, but I'll explain why I think it's fair not to hold Pockit liable for these transactions.

The technical evidence I've seen shows that the disputed payments were made through a device different to the one Miss H says belongs to her and from which she logged into her Pockit account on the day it was set up. Based on this information, I accept that the payments weren't made from Miss H's usual device.

But this isn't conclusive evidence that the payments in question were therefore unauthorised. While it's possible that the use of another device could indicate unauthorised access, it's also possible that the customer has accessed their account from another device, for example if they've got more than one device. It's also possible that the customer has let someone else access their account from that individual's device, either willingly or through deception.

Pockit has explained that several pieces of information are needed for a new device to gain access to a customer's account: the secret question needs to be answered, a one-time passcode (OTP) sent to the registered phone number needs to be entered, and a 'magic link' sent via email to the customer's registered email address needs to be clicked on. In this case, Pockit has said that the OTP and the magic link were sent to the contact details Miss H provided at the time of opening the account.

Miss H says she had nothing to do with the disputed payments, and she's offered explanations for how a third party could have obtained the information that was needed in order to gain access to her account to make them. This includes: temporarily losing her phone on the day the OTP was sent, losing her wallet containing documents which a fraudster could have used to guess her phone's password , her iCloud account – which contained personal login information in her notes – being hacked months prior, as well as her email account being accessed remotely to forward the magic link.

Where evidence is incomplete, missing, or contradictory, I need to determine what I think is more likely than not to have happened. I do this by weighing up what I do have and making a finding on the balance of probabilities.

The crux of Miss H's complaint is that she believes Pockit should have refunded the two payments she says were unauthorised under the Payment Services Regulations 2017. As I've already mentioned, I'm satisfied that the payments were made from a different device to the one Miss H used to set up the Pockit account. But the difficulty I have is that while her explanation for how individual pieces of information could have been compromised is

possible, I'm not convinced by the overall plausibility of what she says happened such that this is more likely than not to be what did happen.

For instance, Miss H says she lost her phone in town on 28 April, and it was subsequently found in the dressing room of a clothes store. She says the phone was not in her possession when the OTP was sent, and that she noticed the message later on when she was reunited with it. But the OTP was sent in the early hours of 28 April, at around 1:30 am, whereas her testimony is that she lost her phone while visiting the town centre and trying on clothes. Based on the timing of events, I consider that the new device was set up before Miss H says she lost her phone.

Similarly, Miss H says the fraudster remotely accessed her email account and forwarded the magic link within minutes of it being received. From what she's told us, her iCloud was hacked into a few months prior, and she took steps at the time to secure her details. In the circumstances, this previous incident doesn't appear related to how the secure information needed to set up the new device could have been compromised. I also think it's extremely unlikely that an unknown third party who hacked Miss H's iCloud months prior to the disputed payments would also come upon her mobile phone to access the OTP or emails, especially when she's told us she's not disclosed any information to anyone.

In questioning the plausibility of Miss H's explanation, I'm mindful that the account activity log I've seen for 2 May – when the payments happened – shows logins from her device in between the two payments made from the other device. And following the second payment, Miss H doesn't transfer the remaining balance until a further 30 minutes.

Additionally, I can't see that Miss H contacted Pockit about the disputed payments until a few days later. Nor did she report suspicious activity when Pockit sent emails to verify account logins from the other device prior to the payments. In my view, the actions or lack thereof are not consistent with a claim that there was unauthorised access on the account.

Then, there's also Miss H telling Pockit that she made the payments in relation to a job opportunity. I acknowledge that she now says she got the details mixed up. But I find it strange that in getting the details mixed up, Miss H was very specific to Pockit about what led her to making each payment that she's now disputing as unauthorised.

I think there might be more going on that led to these payments than what Miss H has told us. But I'm satisfied that we've given her an opportunity to tell us what exactly happened. As she maintains that she was not involved whatsoever, and I'm not persuaded that that's the case here, I don't think Pockit has acted unfairly in holding Miss H liable for these transactions. Although there could have been third party access, on balance, I'm not persuaded that this was without Miss H's knowledge or consent.

My final decision

For the reasons given, 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 H to accept or reject my decision before 11 May 2026.

Gagandeep Singh
Ombudsman