DRN-4113677

The complaint

Miss W complained because Metro Bank PLC refused to refund her for transactions which she said her then-boyfriend had made.

What happened

On the night of 7/8 September 2022, Miss W was at home with her boyfriend, who she'd been with for two years. She made an online banking payment for a course, and at the time she didn't realise that her boyfriend, who was taller, was looking over her shoulder to see her passcode for her online banking.

When Miss W woke up around 8am, she went onto her online banking to transfer some money from her savings account. She noticed that money had been stolen from her account overnight, and transferred to accounts she didn't recognise. Miss W confronted her boyfriend, because no-one else had access to her devices apart from him. She rang Metro, and asked it to reverse the outward payments. Metro told her this wasn't possible, because some payments take 24 hours to leave an account. Metro's adviser told her there was nothing he could do.

Miss W's boyfriend had taken her phone when she was asleep. He'd then transferred £10,000 from her savings account to her current account, and had then carried out payments from her current account. Four faster payments had been made in this way, totalling £7,500.

Miss W rang again, and also went to a Metro branch and to the police.

In the call between Miss W and the fraud team on the morning of 8 September, Metro said that its security systems had flagged and blocked two of the faster payments: one for £2,500 and one for £500. Another £2,500 payment didn't go through to the recipient account. This left an outstanding amount of £2,000, which had been paid out from Miss W's account. It had gone to the same payee as the £500 which had been blocked.

Metro told Miss W that Metro expected customers to have a certain level of security on their phone, so it wouldn't be able to refund Miss W. It said that to log in, the person carrying out the payments would have needed Miss W's 12 digit customer number, three digits from her security number, and three characters from her password.

Miss W complained. She set out what had happened, and said that it wasn't correct that all this information would have been needed. She said that when she usually sent money, the app only asked for the passcode, and then sent her a one-time passcode when entering a new payee, which was sent as a text to her mobile.

In its final response letter, Metro told Miss W that it couldn't refund her for the lost £2,000 because the payments had been made using the correct security information. Metro again said that log in would have needed the 12 digit customer number, three digits from her security number, and three characters from her password. Metro pointed out that the mobile used had been consistently used for genuine payments, and a one-time passcode, sent to

the mobile, was required before the new payees could be set up. It said that as Miss W knew who had made the payments, it was a police matter.

Miss W didn't agree, and contacted this service.

Our investigator upheld Miss W's complaint. He said that Metro should have raised a fraud case when Miss W had first phoned, and hadn't done so. This meant that Metro's response to the fraud report was delayed. The investigator also said that Metro, and Miss W, had different versions of what was needed to set up a new payee. Metro hadn't provided evidence of what security had been passed to set up the new payees on the app, but had said there were different requirements according to whether a new payment was set up using mobile or online banking. Miss W's boyfriend had accessed her app, and set up new payees and made the payments without her authority, after learning her eight digit PIN. The investigator said Metro should refund the disputed £2,000, with 8% simple interest from 8 September 2022 to the date of payment.

Metro didn't agree. It said:

- its concern was when does the customer take any responsibility for keeping their account secure? This was a requirement under the terms and conditions;
- access to the mobile, and then to the Metro app on the mobile which needed security depending on the customer's setup. Then a one-time passcode would have been sent to the mobile;
- Metro believed that either Miss W had colluded or hadn't kept her security details safely;
- Metro said that moving money from one of Miss W's accounts to the other didn't raise an alarm with its detection systems. It said that its systems couldn't prevent and question all payments leaving a customer's account;
- Metro said that if Miss W believed that her boyfriend had seen her security details, she'd been grossly negligent as she'd failed to conceal the details.

Metro 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.

Regulations and authorisation

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.''*

I note that Metro and Miss W disagree about exactly what would have been needed to authenticate the payments. But it doesn't make any difference whether it would just have needed the passcode, or other information as well. That's because the issues relate to Miss W's boyfriend being able to discover whatever was needed by watching her carry out a genuine transaction, not to exactly how many pieces of information he'd have needed.

Miss W says she didn't authorise the four faster payments from her current account, nor the £10,000 transfer from her savings into her current account which enabled the payments to

be made. Metro has suggested to this service that Miss W might have colluded in the payments, and I've carefully considered this possibility.

I've listened to the phone call recordings which we have, though these don't include Miss W's first call to Metro. Both sides agree that on that occasion she was told that payments would take 24 hours to go through, and the fraud team wasn't alerted. Having listened to the other calls, I consider it's more likely than not that Miss W didn't collude, and that the transactions were, as she reported, genuinely carried out by her boyfriend without Miss W's consent. I've also borne in mind that Miss W reported the dispute quickly and was consistent throughout. She also pursued this consistently, including going to the branch, and reporting it to the police and Action Fraud. So I find that it's more likely than not that the events happened as Miss W reported, and she wasn't acting fraudulently herself.

Gross negligence

Under the Regulations, a customer is liable for losses if they've acted with gross negligence. Gross negligence isn't defined in the regulations, but Regulation 72 deals with the customer's obligations in relation to security, and says that a payment service user must: ''*..take all reasonable steps to keep safe personalised security credentials relating to a payment instrument or and account information service.''*

There have been legal cases about what ''*gross negligence''* is, and it's been established that it is to a higher standard than the common law standard of negligence. The Financial Conduct Authority (FCA) says it is ''*a very significant level''* and the judge in one of the key cases said that gross negligence isn't just actual appreciation of risk, but serious disregard of risk.

It's perfectly reasonable to complete transactions with other people in the vicinity – it happens at cashpoints, for instance. So someone seeing isn't enough to count as gross negligence. Here, Miss W didn't realise at the time that her boyfriend was watching and had seen and memorised her password, so there was no reason for her to think she should change it, or be concerned. I also wouldn't expect her to feel it was necessary to hide her phone away at night from her then partner of two years, whom – at that time - she trusted.

I recognised Metro's concerns about when does the customer take any responsibility for keeping their account secure, which is required under the terms and conditions. But ''*gross negligence''* is a high bar, and I don't consider that Miss W was grossly negligent in all the circumstances here.

Did Metro act quickly enough, and should it have stopped the payments?

Metro provided poor service to Miss W when the first adviser failed to refer her first call to its fraud department. Metro hasn't provided us with this call, but it accepted that its adviser should have raised a fraud case at that point and didn't do so. This meant that Miss W had to ring again, and it lengthened the time when she was anxious about what to do. I've also looked at whether it would have made any difference if Metro had acted correctly and referred Miss W's situation to its fraud team when she first alerted them.

I don't have the call or the time it was made, but as Miss W's boyfriend carried out the transactions when she was asleep, her call would have made been some hours after the transactions had taken place. That wasn't Miss W's fault, but faster payments go through within minutes, almost immediately. So even if Metro's adviser had acted correctly, it would have been too late to stop the payments by then anyway.

I've then looked at whether Metro's systems should have blocked all the payments on security grounds before they were paid, on grounds that they were out of character for Miss W's account.

Looking at Miss W's statements from January 2022, I find that the disputed transactions were out of character. Her spend was almost all by card payment, with a very occasional direct debit. I haven't seen any other faster payments. Her card payment spend was generally under £40, with very occasional higher amounts eg £159 to a supermarket in April, and another payment for £352 in June. So payments which were faster payments, and for £500, £2,500 and £2,000, were very much out of character.

Looking at transfers between accounts, Miss W did many transfers between her accounts. The amounts she transferred were typically higher than her card payment spend. The highest I've seen was for just over £1,000, but this was still considerably less than the £10,000 transfer into her current account which was then almost emptied immediately. Fraudulent payments from an account are often preceded by a substantial transfer from a savings account into an account from which outgoing payments can be more easily made – which is what happened here. So I think the large transfer into the account, followed by the large transfers out, should have triggered security alerts.

It looks inconsistent that Metro's systems did flag and block two of the payments (and one failed or an unknown reason) - but its systems didn't flag and block the £2,000 payment. That payment was to the same recipient as the £500 payment which had been blocked. Banks don't provide details of their security systems, and algorithms are complicated. But I find it surprising that the system blocked a £500 payment to a beneficiary, but then let through a £2,000 payment to the same recipient. I consider that Metro should have flagged and blocked that payment too. And sending a one time passcode, when a suspect mobile transaction might well be under the control of a fraudster, is never going to be entirely satisfactory as verification.

Conclusions about the outstanding £2,000

So I consider that:

- It's very unlikely that Miss W colluded with her then-boyfriend as Metro has suggested. I accept that she didn't know about the payments, and didn't authorise them. As a result, she was entitled to a refund.

- The circumstances under which Miss W's then-partner obtained her security information, and her phone, are not sufficient to count as gross negligence.

- Metro failed to keep Miss W's money secure by not flagging and blocking all the disputed payments, which were out of character for her account. It did flag two of them, and I consider it should also have blocked the £2,000 payment until it could speak to Miss W in person (not just send a one-time passcode to the phone). It was to the same recipient as the £500 payment which had been properly blocked only a short time before – it was just for a larger amount. And there had also been an out of character large incoming transfer shortly before the large disputed payments.

Taking into account all these factors, I order Metro to pay Miss W £2,000, plus interest at 8% simple from 8 September 2022 to the date of payment.

My final decision

My final decision is that I uphold Miss W's complaint.

I order Metro Bank PLC to pay Miss W £2,000, plus interest at 8% simple from 8 September 2022 to the date of payment.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss W to accept or reject my decision before 1 August 2023.

Belinda Knight
Ombudsman