DRN-4508835

The complaint

Miss M complains that The Royal Bank of Scotland Plc ("RBS") failed to refund a transaction she didn't recognise.

What happened

Miss M became aware that a large (£1,700) bank transfer had been made from her account that she didn't recognise. She contacted RBS about this payment. During the investigation Miss M explained that she'd changed the security settings on her phone whilst she was at work (where the disputed transaction had taken place).

Miss M described how she'd removed the phones security in order to make it easier to use her phone whilst working. She further explained it was kept in an unlocked cupboard and her banking security details were written down in an unprotected file on her phone.

She believed that someone had accessed her unlocked phone and obtained her logon details for her banking app to set up a bank transfer.

RBS looked into the situation and thought that whilst Miss M hadn't made the payment herself, she had breached the terms of the account by leaving her phone unprotected with banking information available on it. RBS declined to refund Miss M.

Miss M raised a complaint with RBS who again looked into the circumstances of her loss. They didn't change their position and Miss M brought her complaint to the Financial Ombudsman Service for an independent review.

An investigator was assigned to look into Miss M's complaint and asked both parties for information about the disputed transaction.

Miss M confirmed the circumstances of the loss of her funds, further explaining that:

- Biometrics and personal identification number (PIN) were set up with her phone but switched off whilst at work due to difficulties working in a darkened room.
- She didn't recognise the payee who received her funds.
- She didn't believe anyone else had access to her phone.
- The loss wasn't reported to the police.
- The lost funds were from savings.
- Miss M couldn't explain how it happened but was only working or at home at the time.
- She never lost her phone.

RBS provided details about the transactions and extracts from the agreement they had with Miss M about the operation of her account.

RBS explained that Miss M's account was accessed using her banking credentials issued to her and a transfer was made from one of her other accounts into her "Foundation" account".

Facial recognition was then added to her banking app and a new payee was set up. £1,700 was then transferred from her account to the new payee.

After considering the evidence, the investigator didn't think that RBS needed to do anything and Miss M's complaint wasn't upheld. In summary, the investigator said:

- RBS accepted that Miss M wasn't responsible herself for the transaction.
- Miss M failed to take reasonable steps to protect her mobile device/banking information.
- Miss M was in breach of the terms of her account and was in effect negligent.

Miss M disagreed with the investigator's outcome and argued that as she hadn't made the payment herself, she shouldn't be held responsible for it. She said that she wasn't logged into her banking at the time and the payment wasn't her fault.

She later said that no one knows her banking password and she wasn't responsible for the facial recognition being set up.

As no agreement could be reached between the parties, the complaint has now been passed to me for a 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.

Miss M's version of events is that she unlocked her phone whilst at work but left it in an open cupboard in a work room. Her banking details were kept in an unprotected part of her phone (the notes section) and this is how a third party was able to use her phone to gain access to her account and transfer the funds from it. She later said that no one else knew her banking password – by this I've taken it that she hadn't told anyone about it or given it to someone deliberately.

RBS accepted Miss M wasn't responsible for the payment herself but was in breach of the terms of the account.

The regulations relevant to this complaint are the Payment Service Regulations 2017 (PSRs) and specifically:

Section 72 - ***Obligations of the payment service user in relation to payment instruments and personalised security credentials***

72.—*(1) A payment service user to whom a payment instrument has been issued must—*

(a)use the payment instrument in accordance with the terms and conditions governing its issue and use; and

(b)notify the payment service provider in the agreed manner and without undue delay on

becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument.

(2) Paragraph (1)(a) applies only in relation to terms and conditions that are objective, non-discriminatory and proportionate.

(3) The payment service user must take all reasonable steps to keep safe personalised security credentials relating to a payment instrument or an account information service.

Essentially this says that the payment service user (Miss M) must use the payment instrument (which includes the banking app) in accordance with the terms and conditions of the account (assuming those terms don't fail para (2)). Also, that Miss M must keep her security details safe.

RBS's terms for the use of the account go on to specify that:

5 Keeping your account safe and limiting the use of your account

5.1 What you need to do to keep your account safe

You must:

- *take all reasonable steps to keep your security details safe (including your debit card PIN and any passwords or log-in details for telephone, mobile or online banking);*

- *… you must make sure that any information stored or displayed on your device is kept secure;*

Miss M agreed to these terms when she opened the account and having considered the section of the terms relevant to this complaint (set out above), I don't think they fail the test set out in 72 (2). By that I mean that the requirements to keep her security credentials and any device used for banking (including her phone) safe and secure is a fair and reasonable term.

RBS believe that Miss M was in breach of these terms by her actions when she took off the phone security and recorded her banking details in an unprotected part of her phone. This falls under the gross negligence test. This means that RBS have to show that Miss M failed with gross negligence to comply with her obligations as a payment service user, which allowed the disputed transaction to take place.

It's generally held that gross negligence is a lack of care significantly beyond what's expected from a reasonable person. The Financial Conduct Authority (FCA) interpret it as "… *have shown a very significant degree of carelessness*"

So, in order to determine if Miss M can be held liable for the payment due to her actions, I have to consider the steps she took with her phone and how she recorded the banking details.

She's already explained the circumstances for taking off the security on her phone due to working in a dark room. Whilst I can understand how the light level could possibly affect facial id (although it's designed to work in such light levels), I don't understand why the PIN couldn't have been used. I doubt this would be affected by the room she worked in. But, taking the decision to remove all the protections from her phone meant that anyone could access it.

By then recording all her security information on an unprotected part of the phone meant that anyone who had access to it could use it and open up the online banking app to make whatever transactions they wanted to. It's the combination of taking the basic phone protection off and leaving the security details exposed that I think push Miss M's actions into the realm of gross negligence.

I just don't think it's something that a reasonable person would do with their device. Miss M would have been aware that her phone was unprotected and contained all her online banking information, leaving her accounts open for anyone who had access to the phone.

If the phone's security was left on, it would be a different matter because Miss M would have taken reasonable precautions to protect her device and the banking information. But, by removing the phones protection, she effectively left her banking open for anyone who was disposed to take her funds.

I haven't looked further into the facial id set up on her banking as that happened once the various security details had already been obtained from the open phone. But, I thought it unusual for someone who was stealing funds to set up facial id when they already had the password to get into the device.

Overall I think that Miss M's actions left her device unprotected and her banking logon details available for anyone who was able to obtain her phone. This was in breach of the terms of the account, and I'm satisfied that this met the test for gross negligence. So, whilst I have sympathy for the loss of her funds, I don't think it would be fair or reasonable to ask RBS to replace them.

I understand Miss M has the details of the account those funds were sent to, so she's able to report that to the police if she wishes.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss M to accept or reject my decision before 15 February 2024.

David Perry
Ombudsman