DRN-5745847

The complaint

Mrs T complains The Royal Bank of Scotland Plc ("RBS") won't refund transactions made from her current account which she says she didn't make or authorise.

What happened

Mrs T is disputing a total of 55 transactions between November 2023 and April 2024. These payments were made using six different cards that were issued to Mrs T.

RBS said it wouldn't refund the transactions because it couldn't see a point of compromise for Mrs T's card details. Mrs T complained to RBS about this decision, but RBS continued to refuse to refund the transactions to Mrs T.

An Investigator considered Mrs T's complaint. She said, in summary, all but one of the disputed payments had been made using card details either online or by telephone. There was a single point of sale transaction that had been made using Mrs T's card and Personal Identification Number (PIN). The Investigator found, based on what Mrs T had told us, she couldn't see how an unknown third party could have accessed all six of Mrs T's cards – or their details – in order to have made the transactions. So she didn't think RBS had treated Mrs T unfairly by refusing to refund them.

Mrs T didn't accept the Investigator's findings. She said she wanted an Ombudsman to review the matter. So the complaint was passed to me.

I issued a provisional decision. I've set out my findings again below and they form part of this decision.

Provisional findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

Under the Payment Services Regulations 2017, generally, RBS can hold Mrs T liable for the disputed transactions if the evidence suggests that she made or authorised the transactions.

RBS has provided evidence that all but one of the transactions was made online or over the phone. This means whoever made these transactions didn't necessarily need to be in possession of Mrs T's physical card, just the card details i.e. card number, expiry date etc. It also means that all but one of the transactions is a distance contract. A distance contract involves transactions made where the customer is not physically present at a merchant, like telephone or online transactions. The terms and conditions of the account say all unauthorised transactions made "at a distance" will be refunded. So this means the only basis on which Mrs T could be held liable for them is if she authorised them.

Mrs T has told us she keeps her cards in a purse, kept in a handbag in her bedroom. She said she lives alone and no one else has access to her cards or her card information. And

she's never lost or misplaced any bank cards. After each card was used for the disputed activity, Mrs T still had it in her possession.

Mrs T has also told us she'd never given her card details to anyone other than for genuine card payments. She said she'd never given her card details to anyone following requests via text message, email, phone call or a link.

During the period of the disputed use, Mrs T had six different cards. These cards were all issued following unrecognised transactions taking place which RBS contacted Mrs T about. This means that, to have made the transactions in dispute, an unauthorised party would have needed regular access to Mrs T, or her home, to obtain the new card details each time one was issued.

RBS has provided a call recording of a conversation it had with Mrs T on 5 March 2024. In this call, Mrs T mentions having received a call that day from someone who asked for her card details – which she said she gave – on the basis that the caller had told her she was due a refund in relation to some insurance for her fridge-freezer. There's no corresponding refund credited to Mrs T's account around the time of this call based on her statements. Importantly, she said the caller knew about the problems she had been having with the bank – which seems highly unusual if the person had been genuinely calling from an insurer. The agent discusses with Mrs T that this seems likely to be a scam call and likely from the person who has already been making transactions using her card details. During the same conversation, Mrs T mentions her landline hadn't been working for a week and things had been "quiet" as she hadn't received as many calls as she usually does. The agent doesn't probe Mrs T in much detail, but it seems that Mrs T was saying that she does usually receive unsolicited calls.

So despite what Mrs T has told our service and the bank, it seems she told the bank she had disclosed her card details to an unsolicited caller on at least one occasion. And that, despite denials on other occasions, she does receive unsolicited phone calls to her landline – likely from people requesting her card details or other personal information. The repeated calls would make sense if Mrs T is someone who has cooperated with them in the past, the fraudster is likely to continue contacting her.

We asked Mrs T about this call and to tell us more about the calls she was referring to in this conversation. Despite reminders, Mrs T did not respond by the deadline we set.

Based on what Mrs T told us initially, it seemed no one other than Mrs T herself had access to the cards or the card details. So it was difficult to understand how such a high volume of transactions across six different cards was done without Mrs T's involvement.

Although in her submissions to our service Mrs T has been adamant no one other than her had access to the cards or the card details, I don't think this can be correct. Based on the content of the call with RBS on 5 March 2024, I think Mrs T had disclosed her card details on a least one occasion and it seems more likely than not that, given the transactions took place over multiple cards, Mrs T had done that several times in relation to each new card. Which is how the transactions continued to be made.

The evidence shows six of the online transactions were authenticated using 3D Secure (3DS). 3DS is an extra layer of protection as it requires customers to verify their identity during online purchases. But most of the disputed transactions were not authenticated via 3DS. RBS has provided screenshots showing the messages that would have been displayed during the transaction requiring authentication using 3DS. But, since I don't think Mrs T was making these transactions, she wouldn't have seen these screens.

RBS has explained that as Mrs T wasn't registered for online banking at the time, any 3DS transactions would have required the party making the transaction to have entered a One Time Passcode (OTP) which would have been sent to Mrs T's landline number, mobile phone number or email address.

RBS can't though provide evidence of the OTPs being sent to Mrs T's contact information in this case or how they would have been responded to. And Mrs T doesn't recall ever receiving any. But even if RBS could evidence the OTPs, I don't think this makes a difference to the outcome of her complaint. I say this because if Mrs T was willing to disclose her card details to callers, I think it's likely she was also persuaded to disclose any OTPs. Which would explain how the transactions authenticated using 3DS were able to take place.

The online and telephone transactions don't appear to be in keeping with Mrs T's usual spending and RBS' fraud prevention measures did pick up some transactions that Mrs T ultimately said she hadn't made. So overall, I'm satisfied that the online and telephone transactions were unauthorised and should be refunded.

The total value of the transactions in dispute is about £20,000. Mrs T has received some refunds from RBS and from some of the merchants directly, so RBS only need to refund any disputed distance transactions Mrs T hasn't already received a refund for.

Turning to the physical card transaction, this was made on 13 February 2024 at 3:15pm for £19.99 at a well-known high street retailer. RBS has provided evidence Mrs T's genuine card was used and her PIN was entered. I say this because RBS' evidence shows the chip in Mrs T's card was read during the disputed transactions. And it's not generally thought possible to copy the chip on the card. The last undisputed use of Mrs T's card and PIN, before this transaction, was on 10 February 2024 at 12.07pm. So if the card had been cloned, I'd have expected to have seen it used much sooner than 13 February 2024 and repeatedly for much larger amounts, rather than a single low value transaction. Mrs T has told us she had her PIN written down, disguised, but she does keep it in her handbag.

Based on what Mrs T has told us, it seems no one other than Mrs T herself had access to the physical card and PIN. I'm not persuaded it's likely Mrs T was observed entering the PIN on 10 February 2024, the card was then obtained and used by an unauthorised party three days later, before being returned to Mrs T unnoticed. And Mrs T disclosing card details over the phone wouldn't explain how an unauthorised party could have made this particular transaction. So I don't think this transaction was unauthorised like the others. I think it's more likely than not that Mrs T included this one by mistake.

Responses to my provisional decision

Mrs T responded to say she accepted my provisional decision.

RBS responded to say it didn't agree for the following reasons:

- Mrs T hadn't reported the transactions promptly enough as required by the terms and conditions of the account. And Mrs T had been the victim of fraud previously, so RBS felt she ought to have monitored her account more closely.
- RBS accepted its terms say unauthorised distance payment transactions will be refunded, but this was contingent on timely reporting.
- RBS pointed out a genuine transaction had been approved via 3DS using an OTP – which meant Mrs T had received the prompt and acted on it. So she would've done the same with the other transactions approved via 3DS.

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.

RBS has said it feels Mrs T isn't due any further refunds because she didn't report the transactions in a timely manner. The transactions in dispute took place between November 2023 and April 2024. Several fraud claims were raised during that period, and any transactions that were not disputed during those claims had been raised by Mrs T by the time she'd made her complaint in July 2024. So I don't agree that there was such a significant delay that it would be fair or reasonable to refuse a refund on this basis.

RBS also said Mrs T ought to have been monitoring her account more closely as she'd been the victim of fraud in the past. Mrs T did not use online banking, she only had paper statements at the time – which would naturally limit her opportunities to monitor the account. I don't think there was an obligation on her, in these particular circumstances, to do more than monitor her account in the usual way via her monthly statements, despite having been the victim of fraud in the past. And, in any event, as I explained in my provisional decision the transactions in dispute are distance contracts, so Mrs T can only be held liable for them if she authorised them – which I've explained I don't think she did.

RBS has mentioned a genuine transaction being approved via 3DS using an OTP. But still hasn't provided evidence of OTPs being sent to Mrs T. In any event, I explained in my provisional decision why I didn't think this made any difference. And I don't think what RBS has now said changes anything, for the same reasons set out in my provisional findings.

So, my decision remains that I'm satisfied the disputed online and telephone transactions made between November 2023 and April 2024 were unauthorised. The terms and conditions of the account say all unauthorised transactions made "at a distance" will be refunded.

The total value of the transactions in dispute is about £20,000. Mrs T has received some refunds from RBS and from some of the merchants directly, so RBS only need to refund any disputed distance transactions Mrs T hasn't already received a refund for.

Finally, RBS has mentioned referring Mrs T to a Customer Protection Manager who could offer her support with managing her account more securely. RBS should contact Mrs T directly to discuss this with her. And I'd encourage Mrs T to engage with the bank on this.

My final decision

For the reasons I've explained, I uphold this complaint.

To put things right, I require The Royal Bank of Scotland Plc to:

- Refund all the disputed distance transactions made between November 2023 and April 2024 that haven't already been refunded.
- Pay 8% simple interest on the refund from the date it debited the account until the date of settlement. If RBS considers it's obliged to remove tax from this interest, it should tell Mrs T how much it has taken off. RBS should give Mrs T a certificate showing how much tax it's taken off, if she asks for one.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs T to accept or reject my decision before 18 September 2025.

Eleanor Rippengale
Ombudsman