DRN-3212054

The complaint

Ms S complains that The Royal Bank of Scotland Plc recorded information about her with fraud prevention agencies. She says this is unfair and would like this information removed.

What happened

Ms S had a current account and savings accounts with RBS. Ms S has explained that she used her current account to receive her benefit payments.

On 23 April 2020, a benefit payment of just under £1,500 was paid into Ms S's current account. The money was transferred out of Ms S's account in four separate payments on the same day leaving a balance of 38 pence.

On 30 April 2020, three £500 payments were paid into Ms S's current account. These payments were then rapidly transferred out of the account to other accounts.

In early May 2020, RBS received notification from the sending banks that the payments paid into Ms S's account on 30 April 2020 were the result of fraud. After reviewing what happened RBS took the decision to close Ms S's accounts. They also recorded a marker with the national fraud database, CIFAS.

Ms S says she wasn't aware the money paid into her account was fraudulent. She's said that she never made any of the transactions out of her account, wasn't registered for online banking and that someone had stolen her benefit money.

Ms S complained to RBS. She said she wasn't able to open another bank account due to the marker which made it very difficult for her to receive her benefit payments. And asked the bank to refund her benefit payment. RBS said it hadn't done anything wrong. And that in line with banking regulations they have an obligation to report incidents like this to CIFAS. RBS also said Ms S hadn't raised a fraud claim with them in respect of her benefit payment.

Unhappy that the CIFAS marker would remain Ms S referred the complaint to our service. One of our investigators looked at Ms S's complaint and asked her some more questions about what had happened in particular whether Ms S had shared her banking information with anyone or lost her bank card. Ms S said she hadn't lost her bank card or shared her PIN or banking credentials with anyone else. So, she couldn't explain how someone else was able to carry out the transactions on her account. She said she believes that her identity had been stolen.

The investigator explained that to record a marker with CIFAS RBS would have to have reasonable rounds to believe Ms S was involved in fraud or financial crime. She said that the bar for recording a CIFAS marker is a high one. And she'd considered Ms S's explanation of what she'd said had happened, but she didn't think her explanation was plausible. So, she said RBS had acted fairly when it recorded the CIFAS marker.

Ms S disagreed. She said someone had stolen her identity details and managed to commit fraud on her account. She says she's a victim too and RBS should remove the marker.

As no agreement could be reached the matter has come to me to decide.

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.

CIFAS marker

Our investigator outlined in detail the level of evidence required for RBS to record a CIFAS marker against Ms S – so I won't repeat it in detail here. But briefly RBS need to be able to demonstrate that there are reasonable grounds to believe that fraud or financial crime has been committed or attempted. And that Ms S was complicit in this fraud or financial crime. What this means in practice is that RBS must first be able to show that fraudulent funds have entered Ms S's account, whether they are retained or pass through the account. Secondly, the bank will need to have strong evidence to show that the consumer was deliberately dishonest in receiving the fraudulent payment and knew it was, or *might* be, an illegitimate payment. But a marker shouldn't be registered against someone who was unwitting; there should be enough evidence to show deliberate complicity.

So, I need to decide whether RBS had sufficient evidence to meet the standard of proof and load a marker against Ms S. Having looked at all the evidence I'm satisfied they have, and I say this because:

- I've seen evidence from RBS that other banks notified them that the three £500 payments paid into Ms S's account on 30 April 2020 were fraudulent. And that Ms S's account, was used to pass them on – the money was transferred out to third party accounts the same day via online banking.
- Ms S says she wasn't registered for online banking. So, it wasn't her who made the online transfers of her benefit money or moved the fraudulent funds out of her account. But this is contradicted by evidence provided by RBS.
- RBS has provided evidence of it's online banking processes which show that to set up online banking a customer's full name, address, date of birth and account details needed to be provided. The bank would then send a unique customer number either by post or email. Following this an activation code would be sent via text and post. RBS have confirmed that Ms S set up online banking on 30 January 2008. And was re-enrolled on 6 April 2019. The mobile number and address used haven't changed and are the same Ms S has provided to this service. So, I think Ms S was registered for online banking.
- Ms S says she has been the victim of fraud and that an unknown third party took over her accounts. And took her benefit money along with the fraudulent funds paid into her account in April 2020. But for a fraudster to carry out the transactions they would need to be aware of Ms S's unique 10 digit customer number, along with three digits from her PIN and password.
- Ms S has said that she hasn't shared any of her banking information with anyone else, no one has access to her home, and she hasn't written down her PIN or online banking information. And always had possession of her bank card. So, she hasn't provided a plausible explanation for how an unknown third party was able to gain access to all the information needed to make the transactions on her account.
- I also note that a payment of £226 on 23 April 2020, made up of Ms S's benefit money was made using online banking and credited the same account that the fraudulent funds were sent to. This payment mandate was created with the use of a card reader therefore, Ms S's debit card and PIN were also used. This debit card was

sent to the address the bank held on file for Ms S. I think it's unlikely that an unknown third party would be able to gain access to Ms S's home address to take possession of Ms S's bank card without her knowledge or consent in order to make this transaction.

- Other payments made on 23 April 2020, were also made from Ms S's account using RBS's mobile banking app and a new payee was created. For an unknown third party to be able to do this they'd need access to Ms S's mobile phone. And I've not seen any evidence that Ms S lost or had her mobile phone stolen.
- In order to access the mobile app, Ms S's six-digit passcode, or fingerprint/face ID would have been required. For a new payee to be created they'd also need access to Ms S's online banking and Ms S's bank card and PIN. Given the way the transactions involved were made, and that Ms S says she never gave away her security details, it isn't realistically possible for anyone to have made them without her permission.
- The payments on 23 April 2020 were made from an IP address that was also used before the transactions took place. The technical evidence shows that the same IP address was used four days earlier. Therefore, I do not believe the activity was carried out by an opportunistic fraudster. If they had access to the online banking from 19 April, then I would question why they would wait four days to remove any funds from the account and not attempt to do so as soon as they had access to Ms S's account.
- RBS has provided technical evidence that shows Ms S's bank card was used on 30 April 2020 at 11:38am to check the balance of her account. Ms S has said she had possession of her bank card. So, I think it's likely it was Ms S checking her account. At this point the three fraudulent payments had credited her account, and Ms S's benefit money had been spent (having been transferred out of the account on 23 April 2020).
- If Ms S hadn't consented to the transactions and had no knowledge of the activity on her account, I think it's reasonable to expect her to alert the bank. But she didn't do so at the time. I can see that Ms S's account was mainly funded by benefit payments, and that this appeared to be her only source of income, so I find it quite telling that Ms S didn't contact the bank immediately, especially if money she relied on had been taken from her account without her consent. It appears Ms S only contacted the bank once RBS had decided to close her accounts and she discovered the CIFAS marker.

I've thought carefully about what Ms S has said – that she's had her identity stolen, knows nothing about the fraudulent funds and has had her benefit money stolen. Having done so I think it's most unlikely that an unknown third party would pay fraudulent funds into Ms S's account unless they were confident that they would be able to withdraw the money or transfer the funds to another account from which they could withdraw it. Ms S has told us that she never disclosed her banking details to anyone else. And has said that she was in possession of her bank card. So, I can't see how an unknown third party would be able to access her account in order to carry out the transactions on Ms S's account, including the withdrawal of Ms S's benefit money, without her knowledge or consent.

In summary, when I weigh everything up, I'm not persuaded by Ms S's version of events. For the reasons, I've explained, I'm satisfied that RBS had grounds to believe that Ms S was involved in the dispersal of fraudulently obtained funds based on the evidence it had. So, I think it was fair for RBS to register the CIFAS marker and I won't be asking them to remove it.

My final decision

For the reasons I've explained I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms S to accept or reject my decision before 2 February 2022.

Ombudsman