complaint

Ms R complains that TSB Bank plc (TSB) won't refund money she lost when she was the victim of a scam.

background

Ms R received a call in July 2016 from someone she thought was from TSB. Unfortunately, this was actually a fraudster. The fraudster told Ms R the money held with TSB was at risk of fraud and it needed to be moved to protect it. When Ms R complained to our service, she said she was sceptical but the fraudster said he was calling from the same number that was on the back of her card with TSB. Ms R says she checked and this was correct. However, the fraudster was using clever technology to 'spoof' the caller identification so it showed a genuine number for TSB on Ms R's mobile.

The fraudster asked Ms R if she had other accounts and she said she did, with another bank, B, which also had money in it. So the fraudster said he'd arrange for someone in B's fraud department to call her immediately. She then received a call which matched the number on the back of her card with B. But, again, this was a fraudster.

Ms R says she felt like she was in a trance, doing what she was told by the fraudsters. She was persuaded to make a number of transfers using her mobile banking app for the transfers from B. Ms R made several transfers from her TSB account including:

- Moving the money held with TSB into the two current accounts she had with TSB. Then transferring that money, a total of £7,000, to a 'new' account that'd been set up for her with TSB. This included most of the £1,000 overdraft available on one of her current accounts leaving that account overdrawn.
- Moving £10,000 from B to one of the accounts she had with TSB and then transferring this to her 'new' account with B.

But there weren't any new accounts that'd been set up for her. In total, Ms R sent just over £33,700 to the fraudsters from her accounts with TSB and B.

Ms R was also persuaded to apply for a loan for £25,000 from TSB. She says the caller said this was because otherwise the fraudsters would get that too so she had to cover all bases. Ms R says this is what the caller had said about the using the overdraft. Fortunately, Ms R's loan application wasn't accepted before she realised what had really happened.

The fraudsters told Ms R that appointments had been set up for her at TSB and B a few days later to collect her new debit cards. And it was only when she went to her appointment with TSB that she realised what'd happened.

Shortly after Ms R reported the fraud to TSB, it contacted the receiving banks, to try to recover the money. Unfortunately, only a small amount from the TSB transfers was left in the receiving accounts. This has been returned to Ms B.

Ms R asked TSB to pay the money to her and raised concerns including why nothing was picked up by its security systems and how the fraudster knew she had a TSB bank account.

TSB says no error was made - it acted on Ms R's instructions. It makes these points:

- the fraud was only possible because Ms R signed onto a banking app from her registered device to set up the transfers.
- over the time Ms R had her account with it, she'd received and made a number of similarly large transfers so this wasn't such unusual behaviour.
- as Ms R set up two transfers to accounts she hadn't paid before, TSB sent her a text message for each new payee to let her know this had happened and ask her to get it touch if she hadn't set them up. But Ms R didn't call the bank about these messages.

So there was no way for TSB to know Ms R was being scammed. Finally, TSB says it doesn't know how the fraudster obtained her contact details but that this can happen in a number of ways such as intercepted post, computer viruses. So TSB didn't agree to pay any of the money sent to the fraudsters to Ms R, on top of the money it'd recovered.

Ms R is unhappy with this so she brought her complaint to our service. Ms R wants TSB to:

- Refund the money transferred to the fraudsters direct from her TSB accounts.
- Investigate where her money went.
- Improve its detection systems including adding security warnings next to the internet banking log on and transfers screen about spoofing.

One of our adjudicator's looked into this matter and acknowledged that Ms R had been the victim of a cruel scam. He answered a number of Ms R's specific queries but didn't think it'd be fair to make TSB responsible or ask it to do anything further. This is because he felt unable to say that Ms R's loss occurred because of a mistake made by TSB. Our adjudicator agreed that TSB's website doesn't say there's an app that fraudster's can use to change the identity of their phone number when logging into online banking. But he explained that it does say the bank will never ask a customer to:

- make any transaction outside of a branch; or
- authorise a payment or send money into a new account that they haven't set up.

Ms R didn't agree with our adjudicator's opinion. She said the banks should check the payee's name in addition to the sort code and account number for transfers. And, if it had done this here, the transfers would've been blocked from going to an account which wasn't in her name. Our adjudicator replied to Ms R to explain that banks are only required to match the account number and sort code on a transfer, not the payee's name. And, as our service isn't the regulator, we can't require a bank to do this. Ms R refers to a super complaint made to the regulator about how banks should change what they do to reduce scams like this.

The complaint has now been passed to me for a decision. Although Ms R has complained about both TSB and B, this decision only looks at the actions of TSB.

my findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint. Where there's a dispute about what happened, I've based my decision on what I think's most likely to have happened in light of the evidence.

Having done so, I have to tell Ms R that I think our adjudicator has reached the right outcome in this case. I think the adjudicator has set out the position very clearly and thoroughly so there's very little I can add to what the adjudicator has already said.

how did the fraudster know Ms R's contact details?

Unfortunately, I don't think it's likely that we'll ever know the answer to this. As TSB has described, there are many ways a fraudster can obtain this information. And, once the fraudster was speaking to Ms R, it might've been a guess that she had an account with TSB. Even so, I haven't seen any evidence to suggest that this was due to a mistake or error made by TSB.

should TSB refund the money transferred to the fraudsters?

Ms R believed, at the time, that she was taking steps to protect her money. And I have great sympathy for her – she's been the victim of a horrible deception which has resulted in her losing a large sum of money. But I have to decide what responsibility Santander has, if any, for Ms R making the payments to fraudsters.

A bank should generally act on its customer's instructions so, if a customer asks to make a transfer and there's enough money in the account, the bank should complete the request. There's no general duty on a bank to check why the customer's making a transfer or ask specific questions. In fact, customers might be unhappy if too many questions are asked.

The transfers in this case were made as a result of them being authorised by Ms R using her secure information on a registered device. TSB followed its normal procedures when it dealt with these payments. It contacted Ms R to tell her that these payees had been set up. And I can see from Ms R's use of her accounts with TSB that she'd received into and sent out of her accounts quite large amounts of money. So I don't see why TSB would've thought anyone other than Ms R was making these transfers.

It's clear that Ms R was persuaded she was dealing with TSB. As a result she made transfers of her money to the fraudsters. There's no evidence that TSB's systems were breached - and it was clever technology that replicated the bank's phone number. So I don't think TSB should pay Ms R the money sent to the fraudsters.

should TSB add security warnings about spoofing?

Ms R suggests TSB should add warnings next to the internet banking log on about spoofing. This isn't something our service could tell the bank to do because we aren't the regulator. However, TSB sets out on its website thing that the bank will never do which are clearly designed to protect someone from scams like this even though spoofing isn't mentioned.

Even so, I don't think it's practical for a bank to set out all scams on its internet banking log in page or when a transfer is being made. I think there's a risk that it'd be so long that customers wouldn't read it. And I don't think this is likely to have made a difference here. I say this because Ms R felt like she was in a trance, doing what she was told to, convinced that she need to act quickly to protect her money.

should TSB's security system have stopped the payments?

Banks are expected to have in place appropriate security arrangements in order to try to prevent fraud. But, these are a matter for each bank to implement. TSB does have fraud detection systems and procedures in place which take account of what it knows about actual and potential risks. However, the way those security measures are set up is a matter for the

bank and its regulator. It'd reduce their effectiveness for the details of them and how they work to become well known.

Even so, there's also a balance to be achieved between the bank protecting users of its services from fraud and it allowing customers to make the transactions they want as quickly and easily as they want to. As I've explained above, banks should, in general, act on the instructions of their customers. And I think that's what TSB did here.

The requests for the payments were made using Ms R's secure information to sign in to her banking app using her registered device. Text messages were sent to Ms R to let her know that it thought she'd asked it to set up new payees. And one of them had an alert raised to check if it was a genuine transaction which Ms R confirmed it was. So I think it would've reasonably looked to the bank as if they were genuine payments, with the knowledge and authority of Ms R.

should TSB have checked the payee's name?

As our adjudicator has already explained, TSB is only obliged to cross check the account number and sort code, not the payee's name.

Turning now to the super complaint mentioned by Ms R. I appreciate this is an area which the regulator is looking into so that it can decide if further regulation is needed to reduce scams like this one. However, even if the regulator decided to change the obligations placed on a bank when processing a payment, this wouldn't apply looking back to previous transfers before the changes come into effect. This means that the obligations TSB had to comply with in 2016 when processing a transfer wouldn't be affected by any amendment to the obligations TSB has to comply with moving forward.

So I don't think TSB needed to check more than the sort code and account number when processing the transfers. And I don't think the outcome of the super-complaint will affect this in Ms R's case.

did TSB act quickly enough once made aware of the fraud?

TSB acted quickly to try to recover the money once it was told there was a problem. But most of the money had already been withdrawn before Ms R realised the fraud. So I don't think TSB would've recovered more money than it has, even if it'd acted quicker than it did.

summary

I'm sorry Ms R has been the victim of an unpleasant scam. Clearly this isn't fair. But that doesn't mean it'd be fair for TSB to cover the loss she's suffered. It was only possible for the fraudsters to do what they did because of transfers Ms R made and authorised using her mobile banking app. And, for the reasons set out above, I don't think TSB can fairly be held responsible for what happened here.

my final decision

For the above reasons, I don't uphold Ms R's complaint against TSB Bank plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms R to accept or reject my decision before 23 November 2017.

Rebecca Ellis
ombudsman