Complaint

Mr N has complained that Bank of Scotland Plc, trading as 'Halifax', won't refund transactions, which he says he didn't make.

Background

Mr N was abroad from 20 July 2018 to 1 September 2018.

He couldn't access his online banking while he was away. On his return to the UK, he reported the problem to his local branch. The branch told him the bank had suspended his online banking because of suspected fraud.

He found out that between 24 and 27 August 2018, his debit card details had been used for online purchases from several luxury and designer retailers. The transactions totalled £2,185.84.

There was also an online banking application for an overdraft, which the bank declined.

During this period, there were four cash deposits into his account, made in the UK, and totalling £1,345.

There were also a number of bank transfers into his account from third parties, totalling £4,065.

Mr N said he didn't make the online purchases. He said he was abroad and had his card with him. He still had his card when he visited the branch. And he hadn't stored his card details anywhere.

He said he lives with his young son in the UK and no one else has access to his property. When he was abroad, he slept in a room on his own. He left his son in the UK with his brother. He said he never left his card unattended.

He said he didn't know how anyone else could know his card details.

He didn't dispute the cash deposits. He explained that one of the bank transfers came from the sale proceeds from his car. The other transfers came from people he knew, who asked him to give cash gifts to their relatives and friends living in the country he visited.

He asked Halifax for a refund of the disputed transactions.

Halifax investigated his complaint and decided not to refund him for the following reasons:

- his card details were used to make the payments. He said he had the card with him and he hadn't stored the details anywhere. If he didn't make the online purchases, then he must have shared the details with someone else
- he didn't need to be in the UK to make online purchases
- he didn't dispute the cash deposits into his account, which were made in the UK while he was abroad

- Halifax had blocked his card on three occasions after declining some transactions. On each occasion, someone called the bank to unblock the card. It believes the caller was Mr N because he passed all its security checks and sounded like him.

However, Halifax also explained that it had suspended his online banking on 24 August after receiving a request to send a reminder of the online ID and to reset the mobile banking app. Given there was a log in just 24 hours earlier, it thought it unusual he should request a reminder.

Despite this unusual activity, Halifax considered that Mr N was the caller trying to unblock his card and, therefore, that he authorised the disputed payments.

As Mr N didn't agree with Halifax's decision, he asked us to investigate.

Our investigator looked into his complaint and decided not to uphold it. He didn't think the caller was Mr N but he couldn't ignore the fact that the caller had passed all the security checks and gave answers, which only Mr N could know. Our investigator decided that the caller could only know these details if Mr N had shared them with him or allowed him access to his account. For this reason, he concluded that Mr N must have allowed someone to use his card details.

Mr N disagreed with our investigator's view. He's asked for an ombudsman's final decision.

my findings

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

The investigator wrote a detailed view that sets out in full the facts, the relevant regulations, the transactions and the evidence. Mr N and Halifax have read the investigator's view so I won't repeat every detail here, only those that are directly relevant to my decision. However, I can assure both parties that I have read the file, including the evidence, which they have provided. Having done so, my review of the evidence has led me to the same overall conclusions as those reached by the investigator and for broadly the same reasons.

In short, Halifax is required to refund the amount of an unauthorised transaction. The relevant regulations, to this effect, are the Payment Services Regulations 2017 (the PSRs 2017). Mr N says he didn't make the disputed payments and is seeking a refund of that amount. So, my primary concern is to come to a view about whether or not I think Mr N authorised the payments.

Having reviewed the technical evidence, I'm satisfied Mr N's card details were used to make the payments. This evidence shows that the card number and CVV code were used to authenticate the payments. For two retailers, there is also an address match.

But the regulations relevant to this case say that is not, on its own, enough to enable Halifax to hold him liable. So, I also need to think about whether the evidence suggests that it's more likely than not that Mr N consented to the transactions. He doesn't need to know about the purchases to consent to them. He is treated as having consented, even if he's allowed someone else to use his card, or account, for another purpose.

Based on this interpretation, I'm afraid I think he did authorise the payments. I will explain why I've reached this conclusion.

I think it's clear someone else had access to Mr N's account and that this person made the online purchases.

I've listened to the calls made by the person trying to unblock the card. I've also listened to the call from Mr N in branch. In my opinion, the voices are very different. I don't consider they are the same person. The caller knew about the purchases and in one call, he described this account as the one he uses for luxury items. This is clearly untrue, looking at the spending pattern on the account. So, I don't think Mr N made the disputed payments. However, if he shared his details with a third party, or allowed him to use his card details, then, as I've explained, he is treated as having authorised them. I now have to consider whether he shared his card details with someone else.

The caller knew enough about Mr N's account to pass the bank's security checks. Admittedly, the caller could've gleaned most of the answers, such as the last ATM withdrawal and details of a regular payment into the account, from a bank statement – paper or online. Personal details might also be obtained from statements, other post and the internet. I think the caller could even make an educated guess at the branch where the account was opened, as the statements cite the branch name and address.

But, there were two pieces of information, which I don't think the caller would know from a bank statement or from online banking: the date the account was opened and the debit card details – in particular the 'valid from' date and the expiry date, which would be on the card itself.

Yet, Mr N said he had his card with him at all times while he was abroad and he hadn't stored the details anywhere or kept a photocopy. He said no one else had access to his home. However, the caller knew his card details. And he used those details to make the online purchases, keying in the CVV code too. I'm afraid I can only conclude that Mr N shared the details with a third party at some point or he didn't have it with him as he says he did. Alternatively, a third party took the card and returned it to him while he was abroad but Mr N has ruled this out. He said he always had the card. Besides, the calls to unblock the card coincided with the UK log ins, so I think it's more likely this was someone in the UK.

I've also looked at the online banking audit reports for Mr N's account. I can see that someone logged in to his online banking on 24 and 25 August 2018 from IP addresses in the UK. This person requested a reminder for the user ID and asked to reset the mobile banking app. The person also applied unsuccessfully for an overdraft.

This clearly wasn't Mr N. He logged in from an IP address in the country he was visiting. However, to log in the person needed the username, password and three digits from a memorable piece of information, which are selected randomly at each log in. Halifax also said the consumer doesn't type in the digits but selects them from a dropdown menu. This is to reduce the possibility of fraud from key tracking.

None of the disputed transactions was made from online banking. I'm including this evidence to demonstrate that a third party had access to the account and knew a considerable amount of information about Mr N's banking details. As with his card, Mr N said only he knew his log in details and no one else had access to his home. Again, I have to conclude that he must have shared this information with someone else. Alternatively, someone he knew had

access to his home and found the relevant information. But this doesn't fit with what Mr N has told us

There were also four cash deposits in the UK between 20 July and 22 August. Mr N doesn't dispute these transactions. He said the deposits were made by:

- a friend, who asked him to give money to a friend abroad (£840 on 20 July)
- his sister, to buy dollars for clothes (£385 on 20 August)
- his brother, who gave him money to go out (£70 and £50 on 22 August).

According to Halifax's records, all the cash deposits were made at 'immediate cash deposit machines.' Halifax told us that in July/August 2018, the machines would have been accepting cash deposits without the need for a debit card. In August 2018, customers could use the machine by typing the sort code and account number only.

At the very least, it looks as if Mr N left his bank details with one or more sibling and or a friend. Admittedly, his account details are not the same as his card details. But I think the evidence shows it's more likely than not that he also shared his card details with someone he knew, given what the caller knew. And he might have been content for a sibling or friend to use his details to deposit cash. It's also possible he wanted his brother, who was caring for his son while he was abroad, to have access to money for his upkeep. However, I appreciate Mr N hasn't said whether any such arrangements were in place.

I accept Mr N didn't carry out the transactions; but I think that either they were done with his agreement or because he gave his details away.

Considering everything, I find, on balance, that Mr N authorised the disputed payments. It follows that Halifax is entitled to hold him liable for them.

I am sincerely sorry for Mr N. I'm sure he didn't expect someone he knew and trusted to use his card details to buy luxury items. However, by allowing someone else to use his card details, albeit for a different purpose, he is treated as having authorised all transactions.

I am sorry to send disappointing news, but I hope the reasons for my decision are clear and I thank Mr N for his patience while we've investigated his complaint.

My final decision

My final decision is that I am not upholding this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr N to accept or reject my decision before 11 March 2020.

Razia Karim
ombudsman