DRN-4388035

The complaint

Mr R complains that Bank of Scotland plc trading as Halifax ("Halifax") failed to refund transactions he didn't recognise.

What happened

Mr R had difficulties accessing his online account and also noticed that his bank card was missing. He reported this to Halifax and identified a number of payments and cash withdrawals that he didn't recognise.

Mr R believed he'd last had his card a week or so earlier when he'd deposited some cash into his account. He confirmed to Halifax that the card was usually kept in his wallet with his other cards in it but only the Halifax card was missing. He kept the personal identification number (PIN) for it secure (although he said he hardly used the card) and hadn't divulged the PIN or any of his online baking security details to anyone else. Mr R confirmed he hadn't responded to any unusual texts or messages (scam attempts).

Mr R sought a refund from Halifax for the disputed transactions. They looked int the payments and told Mr R they'd been made using both the genuine card issued to him and the PIN.

It was later established that Mr R's online account had been reset and a different phone number added to it.

Halifax declined to refund the disputed transactions because they believed the evidence showed that Mr R was responsible.

Mr R complained to them about their decision, but Halifax didn't change their position, Mr R then brought his complaint to the Financial Ombudsman Service for an independent review. The complaint was assigned to an investigator who asked both parties for information about the loss.

Mr R repeated his version of events and denied having anything to do with the payments. Two of the disputed transactions were made with a betting firm and Mr R said whilst he had an account with them, he hadn't used it for some time. Mr R denied receiving any text from Halifax concerning the change in phone number linked to his account. He believed that the loss of his debit card led to the compromise of his account and the theft of his funds. Mr R also reported the loss to the authorities.

Halifax provided details about the payments and how the online banking had been used to change some of the details, including the phone number linked to the account. They provided details of how the account was accessed leading up to the loss of the funds. This showed that the account phone number had been changed but only after a message had been sent to Mr R's current mobile number. Halifax said that Mr R acknowledged the change of number and IP address data showed that the new phone number used an address previously used by Mr R for one of his other accounts. Based on the lack of evidence showing the account was compromised, Halifax believed they were correct when they

declined to make a refund to Mr R.

Note: IP addresses are a means to identify physical locations that online transactions are connected to and can be the actual physical location or other locations connected to the provider of the data services.

After considering the available evidence, Mr R's complaint wasn't upheld. I've summarised the main points concluded by the investigator's report:

- Mr R hadn't disclosed the PIN to anyone else which was needed for some of the disputed transactions and his genuine card had been used (not a cloned card).

- Mr R's phone was only used by him, and he hadn't lost it. It was protected with a code only he knew and also used biometric security to open it. There's no plausible reason to explain how someone could have used the phone without Mr R's knowledge.

- It was difficult to see how gambling transactions could benefit anyone else as any winnings are only paid to the account they were made from.

- The new number was added after Mr R's current phone had received a message and it had been confirmed as genuine by Mr R.

- Funds had been paid into the account prior to the disputed transactions.

- It was understood that Mr R had access to his (online) account despite his assertion that he couldn't get into it.

Mr R disagreed with the investigator's outcome and submitted further points for consideration:

- The funds paid into his account prior to the disputed transactions were done in order to pay for other regular outgoings.

- He was asleep at the time of the cash withdrawals, and they were made some distance from where he lived.

- He didn't change the phone number and was locked out of his account and unaware of the payments being made from his account.

As no agreement could be reached, 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.

The relevant law surrounding authorisations are the Payment Service Regulations 2017. The basic position is that Halifax can hold Mr R liable for the disputed payments if the evidence suggests that it's more likely than not that he made them or authorised them.

Halifax can only refuse to refund unauthorised payments if it can prove Mr R authorised the transactions, but Halifax cannot say that the use of the card and PIN conclusively proves that the payments were authorised.

Unless Halifax can show that consent has been given, it has no authority to make the payment or to debit Mr R's account and any such transaction must be regarded as unauthorised. To start with, I've seen the bank's technical evidence for the disputed transactions. It shows that the transactions were authenticated using the payment tools issued to Mr R. I'll now need to consider the information provided by both parties to determine whether there's sufficient evidence to hold Mr R responsible for the disputed transactions or not.

The basis for this complaint is that Mr R denies making a number of payments, resulting in a loss of Mr R's funds. Two of the payments were to a gambling merchant and required additional security steps before they were authorised (an online PIN being entered) and the cash withdrawals required both the genuine card issued to Mr R and the PIN for that card.

Mr R has confirmed he no longer had his card but hadn't provided any of his banking security details to anyone else, divulged the PIN or given his phone to anyone else to use. Halifax's data shows the online account was accessed and the phone number changed. In order to do that, someone would have to know the password to unlock Mr R's phone (after obtaining it without his knowledge), and to also know the online banking security information known only to Mr R.

If those were known, then the phone number could be changed after a message was sent to Mr R's phone confirming that the new number was genuine. Considering the various steps required to get into the online account and the different sets of security information known only to Mr R, I've found it difficult to establish a plausible and realistic scenario to explain this.

Additionally, the change to the phone number was carried out from an IP address associated with another account operated by Mr R. This would seem to indicate that whoever carried out the change to the account did it from a location previously used by Mr R.

I've also considered how the account was operated. Mr R said he paid funds into it prior to them leaving his account which were for later business payments. Looking at the accounts history, I can see regular payments made into it to manage the outgoing costs associated with Mr R's business. So, the presence of an incoming payment from another of Mr R's account isn't particularly noteworthy, but there was also another payment that was out of the ordinary. Just prior to the disputed transactions took place, a payment from a crypto currency account was transferred into the account and together with the funds already in there, effectively "funded" the outgoing payments.

The data provided by Halifax does show some unusual activity on Mr R's mobile/online banking and this led to its eventual block. Prior to this and during the period the disputed transactions were made, the account was accessible, although Mr R denies being able to get into it (presumably because he believes unknown third parties had taken it over). There's also evidence that the PIN reminder function was used by whoever had the phone, which happened after changing the number.

Whilst I recognise that some parts of the online activity are unusual (using the PIN reminder), I'm brought back to how someone could access the phone in the first place and obtain the banking details in order to bypass the Halifax security controls on Mr R's online account. I understand Mr R believes it was the loss of his debit card that initiated this, but I'm afraid the possession of that card by itself would be unlikely to give anyone else the necessary information and access to Mr R's phone to compromise the account.

Taken together with the other evidence, including the matching IP address data, the use of a gambling site (which only pays money back to the account holder) and the crypto payment, I

think it's implausible to conclude these transactions weren't authorised without stronger evidence to the contrary. That means I think it's more likely than not that Mr R carried out these transactions himself – or that someone else with consent did so.

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 Mr R to accept or reject my decision before 1 December 2023.

David Perry
Ombudsman