DRN-3709451

The complaint

Mr H complained because Bank of Scotland plc, trading as Halifax, refused to refund him for a transaction he said he didn't make.

What happened

At 7:51 am on 24 July 2021, there was a £999.99 faster payment debit from Mr H's Halifax current account to an online cryptocurrency organisation.

A second attempted faster payment to the same beneficiary a few minutes later, for £2,954, was stopped by Halifax's systems. Halifax blocked Mr H's internet banking.

On 12 August, Mr H rang Halifax because he couldn't make payments. Halifax explained that it had blocked the account because of he attempted £2,954 payment. Mr H said he hadn't made either the £999.99 payment, or the attempted £2,954 payment, to the cryptocurrency organisation.

Halifax didn't accept what Mr H had said. It said it could see that Mr H's internet banking password had been changed before the £999.99 payment to C. Mr H said he hadn't changed it. But Halifax's records showed that it had made a verification call to Mr H's phone, to verify the password change. And it told Mr H that after the password had been changed, Mr H had used his registered mobile device to access online banking. So it didn't agree that any third party fraudster had fraudulently accessed Mr H's account without his knowledge.

Mr H didn't agree. He complained, but in its final response letter Halifax still didn't uphold Mr H's complaint, and it refused to refund him.

Mr H wasn't satisfied and complained to this service. He said he'd never heard of the cryptocurrency organisation, and he said that only people who knew what they were doing would invest £999.99 instead of £1,000. He said he didn't have the funds to invest because he had a large family and supported it with benefits. Mr H said that at the time of the £999.99 disputed payment, he was driving the family across Europe. He said his wife didn't drive which he said proved he hadn't made the payment. Mr H also said that Halifax's information said that whenever you make a payment to a new payee, Halifax would ring you to enter a four-digit code, but he hadn't received that. He said this proved he hadn't made the payment. He said that it says online you have to have an account with cryptocurrency organisation in order to make a deposit – which he didn't have. Mr H said he wanted a refund of the £999.99, an apology from Halifax, and compensation.

Our investigator didn't uphold Mr H's complaint. He explained that:

- the IP address used to change Mr H's password was the same as Mr H had used on 22 and 23 July for undisputed transactions;
- before the disputed transaction, a different type of phone had been added to Mr H's account, and this then made the disputed transaction. But a verification call had been made to Mr H's existing phone, to verify the password change, and there had been text messages to tell him about the activity with his online banking. Mr H's existing

phone was then used to authorise the registration of the extra, different type, of phone;
- Mr H hadn't reported his existing phone lost or stolen before or at the time of the transaction.

The investigator also contacted the cryptocurrency organisation C. And it told him that Mr H had opened an account on the afternoon of 23 July, providing a copy of his driving licence as identification.

So the investigator thought it was most likely that Mr H had carried out the disputed transaction himself.

Mr H wasn't satisfied, and sent several long emails. In summary, he said:
- Halifax information said that whenever a customer made a payment to a new payee, Halifax would call and ask for a four-digit number verification. Mr H sent the call log for his first phone and said this didn't show the verification – so it must have been the newly-added phone which received it. He also hadn't received any texts;
- He asked why he'd deposit £999.99 with the cryptocurrency organisation, not £1,000;
- He'd sent a data subject access request (DSAR) to Halifax and hadn't had a response. He said that would have shown whether or not he'd received calls about the payment;
- He wanted the investigator to provide clear information about when the password was changed; when the new phone was added; when the cryptocurrency account had been opened; and phone call information from Halifax;
- He said he'd got a family member to open an account with the cryptocurrency organisation to see what the process was. He wanted evidence of everything supplied to that organisation for the account in his name, and said if it wasn't provided he'd take legal action.

The investigator replied that the verification call from Halifax was automated, so there was no conversation. He'd seen the verification evidence but it was commercially sensitive so he couldn't pass it on. But the investigator provided timescales and dates for the two phones and the activities on them. The investigator also told Mr H that the cryptocurrency organisation had said that Mr H's driving licence identification had been ''*independently verified.''*

Mr H sent another detailed email. In summary, he said:
- He had a legal right to information and he'd twice submitted a DSAR to Halifax which it hadn't actioned;
- The verification call couldn't be evidence if it didn't show his voice, because anyone could have entered the numbers;
- He wanted the investigator to provide proof that he'd purchased or signed a contract for the type of phone which had been added to the Halifax account;
- He said he wouldn't have bought an expensive new phone and then paid £999.99 into cryptocurrency because he was going on holiday and a holiday for his family wasn't cheap;
- He said cryptocurrency wasn't regulated so there was nothing to stop the cryptocurrency organisation lying to the investigator about whether Mr H had an account;
- It would have been impossible for him to have used the same IP address to make the disputed transaction, because he was in Europe, which he could prove by the evidence he'd sent in.

Mr H asked for an ombudsman's 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.

Regulations

There are regulations which govern disputed transactions. The relevant regulations for disputed transactions taking place in July 2021 are the Payment Services Regulations 2017. These say that the payment service provider (here, Halifax) must show the transaction was authenticated. That's the technical part, and here, the disputed £999.99 transaction was technically authenticated.

The regulations also say that it's necessary to look at whether the card holder authorised the payments. In general terms, the bank is liable if the customer didn't authorise the payments, and the customer is liable if he did authorise them. The regulations also say that account holders can still be liable for unauthorised payments under certain circumstances – for example if they've failed to keep their details secure to such an extent that it can be termed ''*gross negligence.''*

So I've gone on to consider whether or not Mr H authorised the transaction. If he allowed someone to carry out the transaction on his behalf, that would count as Mr H authorising it.

I would also point out that this service takes its decisions on what's more likely than not to have happened. Mr H has said we should provide him with a great deal of very detailed information. Some of that I can't provide to him because it's commercially sensitive information. But much of it is information which I don't need in order to take my decision about what's more likely than not to have happened. For example there's no need for me to have proof that Mr H bought and/or signed a contract for the particular type of phone which carried out the disputed transaction. What matters is that the evidence which I do have shows that on balance, it's more likely than not that events happened in a certain way.

Who authorised the disputed transaction?

Before the disputed transaction, the password on Mr H's internet banking was changed, and the new, extra, phone was added to his account. I've looked carefully at these changes:

- An IP address is a unique geographical computer identifier. The password was changed from an IP address which was the same as Mr H used on 22 July for an undisputed £1,200 payment. So I consider it's likely that Mr H changed the password himself.
- Halifax sent a message to Mr H's existing phone at 12:06 on 22 July, which required him to enter a code before the new phone device could be added to the account and activated. This was an automated system, and didn't require a phone conversation. The new phone was activated.
- I've also seen evidence of text messages sent to Mr H's existing phone number about these changes. Mr H didn't contact Halifax immediately to challenge these.

I recognise that Mr H disputes having received any of the text messages, and says he didn't enter the code to verify the changes. But I've seen the computer evidence which shows these were sent, and verification took place.

Mr H said that his security details weren't stored with any online retailer or service provider, and his phone was password protected. Mr H hadn't reported his phone lost or stolen. So it's hard to see any way in which Mr H's details can have been obtained by a third party fraudster.

So I find that it's most likely that it was Mr H himself who changed his internet banking password, and set up the extra phone, on his account on 22 July. The new password and the new, extra, phone, were used to make the disputed £999.99 transaction on 24 July. I consider the password change and the addition of another phone do not prove that the disputed payment was made by a third party fraudster.

Going on to the recipient cryptocurrency account, in his complaint form Mr H told us that he'd never heard of the cryptocurrency organisation to which the disputed payment was made. But the evidence which that firm sent to us, in response to our investigator's queries, shows that an account was set up in Mr H's name, the day before the disputed transaction. For identification, that new account used Mr H's driving licence as identification, and that driving licence was independently verified. Mr H, in response, said that there was nothing to stop the cryptocurrency organisation lying to the investigator. But I can't see any reason why it would benefit the cryptocurrency organisation to do so.

Mr H has also said that he couldn't have made the disputed transaction because he was abroad on holiday. He provided screen shots of a journey which he said prove this. But Mr H could have given his Halifax account and security information to another person to carry out the disputed transaction for him. By the time Mr H left to go on holiday, there were two phones set up on Mr H's Halifax account, and a cryptocurrency account in his name. For the reasons set out above, I consider it's more likely than not that Mr H verified the phone and set up the cryptocurrency account. And if Mr H gave someone else the necessary security information to carry out the transaction, it counts as Mr H having authorised it. I think that's most likely to be what happened here.

Mr H's Halifax DSAR point

Mr H has said that he's twice requested a Data Subject Access Request from Halifax. That didn't form part of his complaint to Halifax, and isn't dealt with in Halifax's final response letter. This service can't consider matters which a customer hasn't previously raised with their bank, so I can't consider Mr H's complaint that he hasn't had a reply to his requests.

But in any case, it seems that one reason Mr H wanted this was because he said the phone call for verification would prove it hadn't been he who verified the details. But that call was automated, so there wouldn't be any recording of either Mr H's, or any third party fraudster's, voice on the call.

Summary

Taking all these factors into account, I consider it's more likely than not that Mr H authorised the disputed £999.99 transaction himself, and I don't require Halifax to refund him.

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 H to accept or reject my decision before 8 November 2022.

Belinda Knight
Ombudsman