DRN-4407503

The complaint

Mr H complains that Bank of Scotland plc (trading as "Halifax") won't refund transactions totalling around £24,000 made to various cryptocurrency platforms that he says he didn't authorise.

What happened

The details of this complaint are well known to both parties, so I won't repeat everything again here. In brief summary, Mr H says that he discovered multiple payments had been made to cryptocurrency platforms using his Halifax debit card between 22 and 26 April 2023, which he says he didn't authorise.

Mr H disputed the payments with Halifax and said it should have stopped the transactions, but the bank said it wouldn't refund them. Halifax explained that the transactions had been made from Mr H's registered mobile device over the course of four days, so it considered that he had most likely authorised them. Unhappy with this, Mr H referred the matter to our service.

Our investigator didn't uphold the complaint. He was satisfied, based on the evidence Halifax had provided, that Mr H had most likely authorised the transactions. Mr H disagreed, so the matter has been escalated to me to determine.

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.

Having done so, I agree with the conclusions reached by the investigator and have decided not to uphold it. I'll explain why.

The disputed transactions complained about took place in April 2023, so of particular relevance to my decision are the Payment Services Regulations 2017 (PSRs) – which apply to transactions like the ones made using Mr H's debit card.

The PSRs say that a payment transaction is authorised by the payer where they have given their consent to the execution to the payment transaction. Such consent must be given in the form and in accordance with the procedure agreed between the payer and the payment service provider.

Unless the payment service provider can show consent has been given, it has no authority to make a payment or debit the customer's account. Where a payment service user denies having authorised a payment transaction, it is for the payment service provider to prove that the payment transaction in question were authorised by the customer.

Having considered the facts before me as well as the relevant law, the key question I need to determine here is whether it is more likely than not that Mr H authorised the transactions. In other words, I need to decide whether Mr H made the transactions himself or gave

someone permission to do so. This is important because a customer will usually be liable for payments they've authorised and, generally speaking, a bank will be liable for any unauthorised payments.

And having considered all the evidence, I'm satisfied the more likely explanation is that Mr H authorised the payments. I'll explain why.

In this instance, the transactions were made using Mr H's debit card, of which some of the payments were subject to stronger authentication checks through Mr H's device. Halifax has provided evidence to show that these transactions were authorised using Mr H's mobile device that had been previously registered on his account, i.e. it wasn't a newly registered device that was making the payments. Halifax explained that the transactions were authorised using a combination of both One-Time Passcodes sent via SMS as well as through Mr H having to login to his mobile banking app to confirm the transactions.

Mr H says he didn't authorise these payments, and that he doesn't know how they would've been authorised from his device. He said he left his phone unattended for brief periods of time. However, he hasn't said that he shared his phone passcode or mobile banking password with anyone else, and said that he didn't store any of his passwords on his phone. So, it's unclear how an unauthorised third party would have been able to gain access to both his phone and his mobile banking app in order to authorise the payments without his knowledge.

I note that the payments were also made over the course of four days, so it wouldn't have been possible for this to have happened from Mr H's mobile device if he had only left it briefly unattended. Mr H has also said himself that the days he left his phone unattended were not the dates on which the transactions were made. So, it follows that the transactions could not have been reasonably been made on the occasions when he wasn't in possession of his device.

I'm also mindful that payments being made to the cryptocurrency merchants in question can only typically be made from an account or payment card held in the same name as the holder of the cryptocurrency wallet. I note that Mr H also told Halifax that he had authorised previous payments to the cryptocurrency merchant. So, taking everything into account, given Mr H didn't share his debit card, device or online security information with anyone else, the only plausible conclusion is that either Mr H made the transactions himself to send money to his own crypto wallets, or gave his details to somebody else, thereby giving his consent and authority for the payments to be made on his behalf. I appreciate that Mr H disputes this, but there is no other more plausible explanation for how the payments could have otherwise been made.

Halifax has also shown that many of the transactions were funded by several Faster Payments being paid into Mr H's account, at least one of which Mr H said had been sent to him by a friend who he was helping to buy a car (though this has not been corroborated by the person who sent the money). So, it seems that the person who made the disputed payments also knew that money would be crediting Mr H's account, which would be highly unusual in the context of an unauthorised person making opportunistic transactions on a phone left unattended. Mr H also wasn't able to provide Halifax with sufficient proof of entitlement to the funds that had credited his account, one of which has also since been reported to have been fraudulent. So, even if I were to accept that the transactions were unauthorised, it's not clear Mr H has even suffered a loss in these circumstances or would ultimately be entitled to the money.

Mr H says that Halifax should have stopped the transactions to verify them with him. But as I've set out above, Halifax did delay certain transactions and required Mr H to confirm they

were legitimately being made by him by asking him to provide One-Time Passcodes that had been sent to his device, as well as through in-app verification. And given the payments had been authorised using both of these means, Halifax would've had little reason to suspect the transactions were being carried out by someone other than Mr H.

I also acknowledge that the multiple payments being made to cryptocurrency wallets in the space of four days ought to have given Halifax cause for concern that he might have been at risk of losing his money to a scam. But Mr H hasn't given any indication that he's fallen victim to any sort of cryptocurrency scam in this instance, so it's unlikely any form of intervention or scam warning would have prevented the payments from being made either. As a result, I don't think Halifax can fairly or reasonably be held liable for the payments for failing to intervene and provide a scam warning.

I appreciate this will likely come as a disappointment to Mr H, but overall, I'm not persuaded Halifax has acted unfairly in these circumstances.

My final decision

For the reasons given above, 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 22 April 2024.

Jack Ferris
Ombudsman