DRN-5730069

The complaint

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

What happened

On 7 October 2022, Mr S rang Halifax. He said he'd received a text telling him he'd exceeded his credit card limit, so he'd checked and didn't recognise several transactions. He said he'd checked his wallet and didn't have his card. He also told Halifax he'd been reported as a missing person during that time, after being on a night out with friends, and didn't know what had happened.

The disputed transactions were ten payments to a vape company, totalling £3,750, and one to a fashion retailer for £825, making a total in dispute of £4,575. Halifax saw these had been made using chip and PIN. So it asked Mr S if he had written down the PIN, or if anyone knew it. Mr S confirmed it wasn't written down and no-one else knew it. He said they hadn't been drinking excessively, and his phone was protected using his fingerprint.

Halifax stopped Mr S's card and advised him to contact the police.

The next day, 8 October 2022, Mr S contacted Halifax again and said he thought his drink had been spiked during the night out. Halifax also saw that Mr S's PIN had been checked on his mobile banking a minute before the first disputed transaction. Halifax refused to refund Mr S.

In late January 2025, Mr S contacted Halifax to complain about its October 2022 decision not to refund him with the disputed £4,575. He said he'd passed out from his drink being spiked, and he said Halifax should have blocked the disputed transactions which he said was a breach of Halifax's duty to safeguard his account. He said he'd been afraid that the fraudsters, who'd have had access to his wallet, would have targeted him or his family. He said that since then, he'd spoken to someone who worked in another bank, who'd been shocked at Halifax's failure to block the disputed transactions. He also said Halifax's dismissive handling of his case had left him feeling unsupported. He asked for a £4,575 refund, an apology for mishandling his case, and for Halifax to review its systems.

Halifax sent Mr S its final response to his January 2025 complaint on 6 February 2025. It said that in 2022, Mr S had said he still had his mobile, which hadn't left his possession. As it couldn't see how someone else could have got his mobile phone to access his online banking to view his PIN, there wasn't enough evidence to suggest the payments had been fraudulent.

Halifax also said that in 2022, Mr S had said he might have been spiked but wasn't sure. Mr S and Halifax had also discussed the fact that his mobile had been used to access the PIN, when this had fingerprint security, and Mr S had said he couldn't confirm a point of compromise as he'd had his mobile with him at all times. Halifax said that in 2022 it had recommended Mr S should contact the police to ask them to access the merchant's CCTV. It said that Halifax's police liaison team can look into a claim when it receives this from police –

but it had no records of the police contacting it about Mr S's claim. So it couldn't change its original decision.

Mr S wasn't satisfied and contacted this service. He said his colleagues and family had reported him as a missing person that night, even though it hadn't been 24 hours. He said he'd been the victim of a serious crime and the transactions had been out of character for his spend. He said he'd told Halifax in 2022 that he was willing to contact the police if it would mean he got a refund, but said Halifax had said that it wouldn't guarantee a refund if he did contact the police for CCTV. He said there were news items showing scammers could bypass mobile phone security to access banking apps, and fraudsters could also have temporarily stolen his phone while he'd been incapacitated. He said he'd looked up some previous cases with this service where we'd ordered a refund.

Our investigator pointed out that because of the time lapse between the event and Mr S's complaint to Halifax, a lot of the evidence such as audit reports, mobile banking app data etc, was now unavailable. So she explained that she would use the information recorded on Mr S's account when he contacted Halifax in 2022.

She asked Mr S for more information. He said:

- his phone had had a pattern passcode as well as a fingerprint;
- his banking app had been protected by a password and biometrics. He said that he understood that the banking app couldn't identify whether fingerprints had been his, or anyone's fingerprints;
- he'd had other credit cards in the wallet that had been stolen, but those hadn't been accessed. He said those cards hadn't had the functionality to view PINs;
- he hadn't asked for CCTV from the retailers or police in order to provide this to Halifax. He said that Halifax's adviser in 2022 had told him it would be a waste of time to ask for CCTV.

Our investigator didn't uphold Mr S's complaint.

She said that we'd look for a point of compromise to find out how a third party would gain access to Mr S's mobile app, and his credit card, and know his PIN. Mr S had said he'd used a different card during his night out, but it had a different PIN, so this couldn't be a point of compromise. Mr S had also suggested that he might have been shoulder surfed when unlocking his phone with the pattern. But he'd told Halifax at the time that his phone had always been in his possession, so she couldn't see how a third party could have accessed Mr S's phone and viewed his PIN without his knowledge.

The investigator also said that she appreciated that Mr S was unsure about the events that evening as he said his drink was spiked. But if he'd given his PIN to fraudsters under duress, or while under the influence, the Consumer Credit Act 1074 said that a customer is liable to transactions that have been authorised. As the transactions had been carried out using Mr S's card and PIN, she considered they'd been authorised. So Halifax didn't have to refund Mr S.

Mr S didn't agree. He sent a long and detailed objection to the investigator's view. In summary, he said:

- Halifax failed in its duty of care by not flagging the transactions, which were highly unusual for him, and took place in the middle of the night in a different city from where he lived;
- There had been court cases where banks had been found to be at fault;
- Halifax had failed to treat him as vulnerable and provided no meaningful support;
- Halifax's adviser in 2022 had discouraged him from going to the police and had said he might still be found liable even if he did obtain CCTV footage;

- he understood that this services uses a ‘’balance of probabilities’’ test, but the investigator had favoured Halifax;
- he’d been drugged so he hadn’t had control of his phone;
- he said mobile banking apps ‘*’can be accessed through biometric trickery’’*;
- his other cards in his wallet hadn’t been used. He said this meant that Halifax’s app was the only one the fraudsters could exploit;
- he had consulted someone who works in another bank’s fraud department. They’d said the investigator was right to say the Consumer Credit Act doesn’t provide for customers under the influence. But he hadn’t been voluntarily drunk or drugged but had been spiked, and he said the law doesn’t expect customers to suffer fraud when they were unconscious or incapacitated through no fault of their own;
- the investigator said that because of the time between the event and Mr S’s complaint, some evidence was no longer available – which he said was extremely concerning and unfair;
- he was entitled to a refund and unless Halifax was held fully accountable for its clear failures, it would remain complacent and leave others exposed.

Mr S 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.

As I’ve set out above, Mr S has raised multiple points in his submissions to this service. I’ve understood all of those and considered all he’s said and sent us, but in reaching my decision here I’ve focused on what I think is vital to my conclusions.

What the Regulations say

There are regulations which govern disputed transactions. The relevant regulations here are the Payment Services Regulations 2017. In general terms, the bank is liable if the customer didn’t authorise the payments, and the customer is liable if they did authorise them. So what decides the outcome here is whether it’s more likely than not that Mr S, or a third party fraudster unknown to him, carried out the disputed transactions.

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.’’*

Mr S quoted a number of previous Financial Ombudsman Service decisions, and court cases, in his emails to us. I’ve taken account of the relevant legal framework in this decision. But when we consider cases, we look at each one individually, taking into account what would be fair and reasonable in all the relevant circumstances of the case.

Difficulties arising from the timescales in this case

The disputed transactions, and Mr S’s initial report to Halifax, took place on 7 October 2022. Halifax refused to refund him, and its records indicate that it suggested he could contact the police to see whether CCTV was available for the locations of the transactions. Mr S didn’t do so, and he’s since said that Halifax’s adviser told him it would be a waste of time to do so. He complained in January 2025.

Mr S also said that it was ‘*’extremely concerning and unfair’’* that some evidence was no longer available. It’s obviously helpful to have as much information as possible, and I don’t

have as much information as usual about the disputed transactions. But banks can't keep all evidence indefinitely. Importantly, Mr S hasn't satisfactorily explained why he didn't pursue his complaint in 2022 after Halifax's initial refusal of a refund. After that refusal, Mr S didn't complain to Halifax about its decision. Nor did he contact this service.

He's given various reasons for this, including that he was afraid the fraudsters also had his personal details from the stolen wallet and might target him and his family; that he now believes fraudsters could have accessed his fingerprint-protected banking app easily; that he is now in a better place mentally; and that he was told by a contact in another bank's fraud department that he should contact Halifax because of its handling of his case and failure to block the transactions.

I'm not persuaded by Mr S's arguments. He had already contacted Halifax on the day of the disputed transactions, so I can't see that complaining about Halifax's decision to refuse a refund would have put him at any additional risk. He provided no medical evidence about being drugged, or being vulnerable either mentally or in any other way. And the records of the 7 October call to Halifax show that he didn't mention possible vulnerabilities, or spiking, at that point, only raising it later.

So I find it surprising that Mr S didn't complain to Halifax at any point between October 2022 and January 2025. If he hadn't made the disputed transactions, I'd have expected he would have done.

Who is most likely to have authorised the disputed transactions?

Mr S said his card was stolen, so the key point is how Mr S's PIN might have been compromised. He said he hadn't written down, or told anyone his PIN. Halifax's evidence is that Mr S's PIN was accessed on his banking app a minute before the first disputed transaction. So I've considered how any hypothetical third party fraudster might have had access to Mr S's phone and his banking app on that phone.

Mr S's evidence is that his phone was protected both by a pattern passcode and also his fingerprint, and his banking app was protected both by a password and also his fingerprint. Mr S said someone could have seen him enter the pattern, and he also suggested that banking apps can't tell whether a fingerprint was his, or just any fingerprint. He hasn't suggested why the password on his banking app could have been compromised.

I can't know for certain who used the banking app on Mr S's phone to look up his PIN just before the disputed transactions. But on Mr S's evidence about the protection on his phone and app, a fraudster would have had to have used his pattern passcode, a fingerprint (on his theory that the Halifax app didn't distinguish between Mr S's and a fraudster's fingerprint) and a password. I don't consider this is likely.

Mr S told Halifax that he was in possession of his phone throughout. He's since said that as he was spiked, he wasn't aware of what was happening. His evidence on his complaint form to this service was that his phone was '*'temporarily stolen''* from his possession. I don't consider fraudsters would take a phone and then return it. They'd keep it in order to try to maximise their gain, from financial transactions or just the sale of the phone.

I also note that Mr S told Halifax his other cards weren't lost or stolen. It seems very unlikely that a fraudster with access to Mr S's wallet would just have taken and used his Halifax card, especially as Mr S says he had higher credit limits on the other cards. Mr S says that the fact the other cards weren't used, means that Halifax's systems were the only one that fraudsters could exploit. I find this very improbable.

I'm also not persuaded that the reason Mr S didn't contact the police was that Haliax's adviser told him it wouldn't guarantee a refund if he did contact the police for CCTV. Clearly Halifax couldn't guarantee in advance that it would refund Mr S if he did contact the police, because it couldn't know what the police would find or what any CCTV would show. But later, Mr S said that he'd been the victim of a serious crime. So I'd have expected Mr S to have chosen to contact the police about a serious crime.

Taking all these factors into account, I consider it's most likely that Mr S authorised the disputed transactions himself. This means that Halifax doesn't have to refund him.

Whether Halifax should have blocked the disputed transactions

Payment service providers such as Halifax are expected to monitor accounts and payments, in order to counter various risks such as money laundering, the financing of terrorism, and fraud and scams. To do this, payment services providers need to have systems in place to look out for unusual transactions or other signs that might indicate that its customers are at risk. In some circumstances, we'd also expect a payment services provider to have taken additional steps, or made additional checks, before processing a payment. In some cases we'd expect them to decline to make a payment altogether.

But there is also a balance to be struck between the prevention of fraud, and the duty to carry out customers' instructions to make payments.

Payment services providers take their own highly confidential decisions on security, and it wouldn't be right for me to have details of Halifax's complex fraud prevention systems. These also change over time, adapting to current fraud patterns, so Halifax's current systems would probably not be the same as those it used in October 2022. I imagine, however, that payments made by the genuine card with its integral chip, and authenticated using the correct PIN, might be less frequently flagged by fraud prevention systems than some other types of payment. That's because they are intrinsically more secure.

It's arguable that Halifax should have noticed an unusual pattern of payments when multiple payments were made to the same payee in a short timescale. However, I don't think intervention would have prevented them from being made, as I consider it's more likely than not that Mr S authorised them.

Finally, this service doesn't consider banks' procedures and policies. So if Mr S wishes to take further his comments that Halifax should have more robust fraud detection systems, he would need to contact the regulator, the Financial Conduct Authority (FCA).

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 S to accept or reject my decision before 28 October 2025.

Belinda Knight
Ombudsman