

The complaint

Mr O complained because HSBC UK Bank plc refused to refund him for a transaction he said he hadn't authorised.

What happened

At the start of January 2023, Mr O contacted HSBC. He said that he hadn't authorised a £9,350.00 payment from his account on 16 December 2022.

Mr O told HSBC that on the night of 15/16 December, he'd been out with friends to a restaurant, nightclub and party. He believed his drink had been spiked, as he became unconscious for around three hours, and didn't remember anything during that time. Mr O said he suspected someone had taken his phone, which was protected by Face ID, and had used it to make the transaction. He said that when he became conscious again, he'd been given his wallet and had checked it briefly, and said his cards seemed to be there. Mr O collected his phone which was on charge in the room.

A £9,350 payment was made from Mr O's HBC account to a company using banking on his mobile phone, at 7.58 am on the morning of 16 December.

Mr O said he got home about 9.30am. He says that later that same day he realised that his HSBC debit card, and a credit card with another organisation, weren't there. But he didn't report the missing card to HSBC at that point on 16 December. When he did ring HSBC in January, he also said he'd been burgled on 31 December, which he believed that was connected with what had happened on 15/16 December. Mr O also changed his evidence to HSBC on a later phone call, saying he'd been intoxicated, not that his drink had been spiked.

HSBC refused to refund Mr O. It said that Mr O was required to keep his personal security credentials secure, and not share them with anyone. Mr O had confirmed on the phone call that he hadn't shared his details. HSBC said that because of the multiple levels of security which were built into mobile banking logon process, and the information Mr O had provided on the phone call, it wasn't likely that his security details could have been used by anyone without Mr O's knowledge.

Mr O wasn't satisfied and complained. In HSBC's final response to Mr O's complaint, it set out that Mr O had said his phone had been stolen, and that someone had used his Face ID to log onto Mr O's online banking and had made the payment without Mr O's knowledge. Mr O had said the phone had then been given back to him and he hadn't realised a payment had been made.

But HSBC said that the transaction had been carried out using Mr O's security credentials and there had been no security breaches. So it was extremely unlikely that any third party had made the payment. And it said again what it had said in its previous letter – that because of the multiple layers of security built into HSBC's mobile banking logon process, it wasn't likely that Mr O's security details could have been used by anyone without Mr O's knowledge.

Mr O wasn't satisfied and contacted this service. He sent a long letter about what he said had happened, and he said that he wasn't liable and the transaction must be refunded. He said that HSBC had detected and blocked a different fraudulent debit card transaction for a much smaller amount, and that another financial organisation had detected other transactions about the same time – which Mr O said meant that HSBC should have stopped the transaction and must now refund it. He also said that if this service were to find that he had authorised the transaction, the payment would constitute an Authorised Push Payment (APP) and if so, HSBC would have to refund him.

Our investigator didn't uphold Mr O's complaint. She said that Mr O's testimony and his version of events were inconsistent in relation to being intoxicated or that his drink had been spiked. He'd said his phone wasn't on him but nearby. The investigator said she couldn't see how a third party could have got through multiple layers of security to carry out the transaction.

The investigator also pointed out that the disputed transaction took place on 16 December. Mr O had been logging in to his mobile banking regularly – but he didn't report it until January. She said she'd have expected Mr O to have reported it sooner, especially as it was for a large amount. So she didn't think the payment had been made without Mr O's knowledge and consent.

Mr O wasn't satisfied. He said he was shocked by the investigator's comment that under the Payment Services Regulations, he'd be liable for payments he'd authorised, and that payments counted as authorised if the payer has correctly authenticated and consented to it. He said that Face ID could easily be used by a third party by the phone being shown to the face of a person who had no knowledge of what was going on because they were intoxicated. He said he was shocked and the investigator hadn't understood or read his statement, because his phone was sometimes on him and had then been taken from him. In reply to the investigator's comment that she'd have expected him to report it sooner, Mr O said that there had been many fraudulent transactions on both his HSBC account and his account with the other financial organisation.

Mr O also said that if the payment was deemed to have been authorised, he was entitled to a refund as he fell victim to a scam while intoxicated and under duress or coercion. So he said he was entitled to a refund.

Mr O 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.

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. Here, I've seen the technical evidence which shows that the disputed transaction was correctly authenticated technically. So the issue for me to consider is whether it's more likely that Mr O authorised the disputed transaction himself and is liable, or that a third party did so without his authority.

Mr O's version of events has changed over time. He first told HSBC that his drink had been spiked and he was unconscious, and a short time later changed that to say he'd been intoxicated. This is important for Mr O's credibility. It's also relevant because the disputed transaction was carried out on the phone which Mr O had registered to his HSBC account –

and the log-in was protected by Face ID. I'm not persuaded that if Mr O's drink had been spiked and he was unconscious, that Face ID would have worked. But Mr O's later version, that he'd been intoxicated, still doesn't explain why the Face ID test was passed, because I also don't consider Face ID would have worked if Mr O had been asleep or had his eyes closed. So the fact that Mr O's phone was used, and Face ID was correctly passed, makes it very likely that Mr O knew about and consented to the transaction. Other security was also passed in relation to the setting up, and making, of the disputed payment on Mr O's account. Mr O told HSBC that he didn't tell anyone else his security details. So I'm not persuaded that a third party carried out the disputed payment.

If a third party had, as Mr O suggests, somehow carried out the disputed transaction, I can't see why that person would have stopped at one £9,350 transaction when there were more funds available in Mr O's account. Nor can I see why the third party would have returned Mr O's phone to him. It's much more likely that they'd have kept the stolen phone and tried further transactions.

I've also looked at the other activity on Mr O's account. He logged in to his phone many times around and after the disputed transaction on 16 December. He logged into his online banking many times around and after the disputed transaction. So he'd have been aware of the transaction. If Mr O hadn't authorised the disputed transaction, I'd have expected him to contact HSBC urgently as soon as he'd next logged on and seen the transactions on his account. It's not plausible that he'd have waited more than a fortnight, even allowing for Christmas, before doing so.

So I find that it's more likely than not that Mr O authorised the disputed payment himself.

Finally, I'll deal with Mr O's other points. This decision relates solely to Mr O's complaint about HSBC. It isn't relevant to my decision what may or may not have happened with Mr O's account with another organisation, as that doesn't form part of his complaint against HSBC. And the fact that HSBC later blocked a different transaction doesn't change my opinion about what's most likely to have happened with the £9,350 transaction. Indeed, if Mr O had genuinely suffered fraudulent transactions on another account elsewhere, I'd have expected him to be even more likely to have reported the disputed transaction to HSBC more promptly.

After Mr O's claim was turned down, he changed his evidence again. As I've set out above, he said that if he was deemed to have authorised the payment, he was entitled to a refund as he fell victim to an APP scam. An APP is a type of authorised scam where the payer completes the necessary steps to consent and ultimately authorise a transfer of money, for example using a Faster Payment which was used here, in accordance with the Payment Services Regulations. But Mr O's evidence all along to HSBC was that he hadn't authorised the payment himself. It isn't credible for him to change that at this stage, and to say instead that yes he had authorised the payment himself but he was forced to do so by a third party. So I don't accept that what happened here was an APP scam.

So I consider that what's most likely to have happened is that Mr O carried out, and consented to, the disputed payment himself. So HSBC doesn't have 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 O to accept or reject my decision before 2 December 2023.

Belinda Knight
Ombudsman