

The complaint

R, a limited company, has complained that HSBC UK Bank Plc won't refund transactions it says it didn't authorise. Mr G, as director of R, is representing the company.

What happened

One day in autumn 2023, R's HSBC card and PIN were used for around £16,000 of spending. Other cards of R's and Mr G's were also used for similar spending that day.

Mr G reported this as fraudulent early the next day. He explained he went to a party, and his phone was stolen. His and R's cards were kept in the phone cover and all shared the same PIN. He didn't keep any record of the PIN or tell it to anyone. He explained that he initially thought he'd just left his phone at the party by accident, which is why he didn't report his cards missing straight away. He evidenced that he replaced his phone, cards, and ID.

HSBC held R liable for the payments in dispute, mainly as they couldn't think of a likely way that a thief might have learned the PIN.

Our Investigator looked into things independently and didn't uphold the complaint. R appealed, so the complaint's been passed to me to decide.

I sent R and HSBC a provisional decision on 2 January 2025, to explain why I thought the complaint should be upheld. In that decision, I said:

HSBC's technical evidence shows that the payments in dispute used R's genuine card, and the correct PIN. But this is not enough, on its own, for HSBC to hold R liable – they also need to be able to evidence that R consented to the transactions, or that it failed to keep its account safe either intentionally or through acting with gross negligence. Otherwise, HSBC have to refund the transactions.

I've looked into what happened with the other banks involved. On the day in question, another bank's app was accessed and used to view the PIN. The disputed payments began at that bank, then the party making the payments moved onto other accounts. I can see that R and Mr G's PINs were manually set by the user, and Mr G has explained that he set the same PIN across all the accounts involved. It's plausible that someone at the party could have – for example – watched Mr G enter his phone's passcode then taken it, or taken it while it was unlocked, then changed the biometrics to access the other bank's app. So it seems both likely and plausible that someone could've learned the PIN for this account and made the disputed payments without R's consent.

The other two banks involved both found that the disputed activity made that day was unauthorised. One noted that the party trying to use the account had avoided using the secure token, did not respond to their identification requests, and used an IP address which did not match the account's genuine activity. That bank felt assured that this was an account takeover situation.

The disputed activity followed a clear pattern of fraud, involving notably large and rapid spending, mixing cash withdrawals and point of sale payments across multiple accounts to maximise how much could be taken, running the accounts involved up to their spending limits, failed attempts to spend after the cards had been blocked, failed attempts to access the online banking facility, and a potential attempt to clone the card.

Mr G's actions seem consistent with R's account being used without consent. He reported the matter early the following morning, reported it to the police and Action Fraud too, and pursued the retailers involved to try to get evidence of who'd made the payments. He had to call the bank from a different phone, and he's evidenced that he replaced the phone, cards, and ID which were stolen. I can see that, following this, Mr G accessed the online banking facility from a new device. And his testimony has been consistent and plausible. I've not found a good reason to disbelieve him.

As such, I currently think it's most likely that the transactions in dispute were made without R's consent.

I've considered whether R failed to keep its account safe either intentionally or through acting with gross negligence. It may have been careless for Mr G to use the same PIN across multiple accounts, and going forward he should probably set different PINs to lessen the risk of something like this happening again. But gross negligence is a much higher standard than normal negligence. I can't see that R (or Mr G as its director) did anything which quite meets the high bar of gross negligence, nor can I see that R or Mr G were intentionally failing to keep the account safe.

So taking into account everything that's been said and provided so far, I don't think HSBC can hold R liable for the payments in dispute.

I'll talk about the responses below.

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.

HSBC queried how a fraudster would guess that the HSBC accounts had the same PIN as the others. I can see that the disputed activity took place on the accounts with the other banks first, before HSBC; so if a fraudster had already discovered that the PINs were the same for those, then it makes sense that they'd try the same PIN for HSBC.

HSBC also queried why a fraudster didn't check the HSBC app. I can't say for certain, but I can see the other banks' apps were used and that the PIN was viewed. So a fraudster would already have got that information. And I can see that payments of various types and amounts were used to try to empty the business account.

HSBC pointed out that Mr G has not changed the accounts' PINs following the fraud, which they felt meant they weren't the same or that Mr G had been grossly negligent. I don't see how this shows that the PINs were not matching before. Mr G's testimony has been consistent and credible about this, I can see the PINs were set by the user, and Mr G never claimed to have changed them since. As I noted in the provisional decision, Mr G should really set different PINs now. But a failure to do so now cannot retrospectively make him grossly negligent in the past.

HSBC suggested that Mr G kept a viewable record of the PINs. But that's entirely assumptive – there's no evidence which shows or substantiates that, and again Mr G's testimony has been consistent and plausible. And as discussed in the provisional decision, there's a likely and plausible way the PIN was compromised without the necessity for any record to have been kept. So I have no reasonable basis on which to definitively conclude that such a record existed or was used.

HSBC argued they're not liable for the transactions because R's PIN was viewed through another bank's app. It's unclear what they're basing this on. HSBC are still liable for refunding unauthorised payments, and I've found these payments to have most likely been unauthorised. This is the case regardless of which app the PIN was viewed in.

HSBC queried why Mr G didn't report things earlier when he noticed his phone was missing, not least as our Investigator mentioned he got an email about one of the payments in the afternoon. To clarify, "evening" would more accurately classify the time of that notification, and I can see Mr G began reporting things to the banks involved that same evening. So I can't fairly conclude that there was a significant undue delay, not least given that there were multiple firms involved. And Mr G has already explained that as the party was at a friend's place, at first he naturally thought he'd left his phone there by accident and thought he would simply pick it up from his friend's place later. That makes sense.

Similarly, HSBC noted the Investigator implied that the cards on another bank's accounts may have used different PINs. But the Investigator hadn't received any information from that bank yet at that point, so I'm unsure why they implied that. I do appreciate that may have been confusing to read, but to clarify they did not have any evidential basis on which to conclude that those PINs were different, which is still the case now.

HSBC felt the person making the payments did so too slowly. I don't agree. When cross referencing the activity across all the accounts involved, I can see that the payment attempts were quite frantic. The activity across the multiple accounts involved notably large and rapid spending, moving from location to location, mixing cash withdrawals and point of sale payments across multiple accounts to maximise how much could be taken, running the accounts involved up to their spending limits, failed attempts to access the online banking facility, and a potential attempt to clone the card. Given how much this party was attempting to drain from all the other accounts, I can see how they might not have got around to using the HSBC personal account. And I can see they did make failed attempts to spend after the cards had been blocked. This is all consistent with a clear pattern of fraud.

Further, as noted before, the other banks involved found that the activity that day was unauthorised. One noted that the party trying to use the account had avoided using the secure token, did not respond to their identification requests, and used an IP address which did not match the account's genuine activity. That bank felt assured that this was an account takeover situation. And Mr G's actions are consistent with this – including reporting this to the authorities, pursuing the retailers, making efforts to identify the party using the card, having to use a different phone, replacing the lost items, accessing his online banking from a new device going forward, and giving plausible and consistent testimony.

Finally, HSBC felt that Mr G didn't come across sufficiently upset when he called them. But I cannot fairly or reasonably hold R liable for these transactions on the basis that its director dealt with the bank too calmly, not least given the weight of all the other evidence I went through above.

On the other hand, R thanked us for the provisional decision. Mr G explained that the disputed payments had greatly damaged R to the point it's facing liquidation, and so he'd had to inject his own funds into the company and spend a lot of his own time and energy sorting things out. He asked whether a portion of the redress could be paid to him directly.

I do understand where Mr G is coming from and I do sympathise with him. I should explain that it's the fraudster who's primarily responsible for their own fraud and for the effects of that, rather than HSBC. It's just that HSBC are liable for unauthorised payments based on the relevant rules. And while HSBC did decline R's claim, this was a very finely balanced case. So I don't think it was wholly unreasonable for HSBC to turn down the claim at first – not least given that they didn't have access to the key information from other banks which I have access to. Further, I cannot say for certain what would've happened to R or how well the business would have run but for the fraud or but for HSBC turning down its claim, and we cannot be too speculative.

When a customer has been deprived of the use of their money, like here, we usually award simple interest onto that money, at the rate of 8% simple a year. This is the same rate that courts use in similar situations, and is sometimes known as statutory interest. Since we don't know for certain what would've happened to R if it'd had that money, I think it's reasonable to use this statutory rate to compensate it.

Turning to who should be paid, I can only award compensation to the eligible complainant, which here is the limited company R. For the purposes of this case, Mr G's involvement is only as a representative of R. We cannot award Mr G personal compensation in a complaint from the company about the company's account. And I'm afraid we can't tell HSBC to pay him directly, as he is not the complainant here.

So having reconsidered the case, I've come to the same conclusion as before, for the reasons set out in this section and in my provisional decision above.

Putting things right

I direct HSBC UK Bank Plc to:

- refund the disputed transactions to R; and-

- pay simple interest to R on those transactions, at the rate of 8% simple a year, payable from the date they were last debited until the date they're returned. This is to compensate R for the time it was without its money.

If HSBC considers that they're required by HM Revenue & Customs (HMRC) to deduct tax from that simple interest, they should tell R how much tax they've taken off. They should also give R a tax deduction certificate if it asks for one. R may be able to reclaim the tax from HMRC if it doesn't normally pay tax.

My final decision

I uphold R's complaint, and direct HSBC UK Bank Plc to put things right in the way I set out above.

If R accepts the final decision, HSBC UK Bank Plc must carry out the redress within 28 days of the date our service notifies it of the acceptance.

Under the rules of the Financial Ombudsman Service, I'm required to ask R to accept or reject my decision before 12 February 2025.

Adam Charles
Ombudsman