

The complaint

Miss B complains that HSBC UK Bank Plc failed to refund transactions she didn't recognise.

What happened

Miss B explained that she was moving to another country and was involved in a life changing accident that caused her to be in a coma for several months. The accident took place in June 2023 and Miss B was in a coma until early December 2023. She reported that when she woke up, she realised her HSBC account had been emptied and a number of her personal items had been stolen, including cards for multiple bank accounts and her phone.

Miss B reported this to the local police who later arrested a person for the theft. A report provided by Miss B showed that the police found her mobile phone and some other items, was returned to her.

Miss B reported the loss of her funds to HSBC and sought a refund of around £24,000. Miss B told HSBC that she needed funds for her and her children to get home. HSBC provided a temporary refund of £4,000 to Miss B. She later said this wasn't enough to pay for her accommodation, her emergency passport expenses and flight tickets for all of them.

The temporary refund was transferred out of Miss B's account the same day and HSBC later advised her that they were taking it back as they believed she was responsible for all the transactions she'd disputed.

Miss B made a complaint to HSBC about their decision not to refund her. They investigated the situation and wrote to a number of merchants involved in the claim made by Miss B. One of the merchants (WU) responded to HSBC's enquiry and informed them that a money transfer (made to the country where Miss B was living) had been completed during the time Miss B was in hospital. The details of the transfer matched Miss B's name and used an IP address that had been recorded previously for undisputed uses of her HSBC account. Miss B later suggested that an ex-partner was responsible for asking her family for payments.

Note: IP addresses are a means to identify physical locations that online transactions/devices are connected to and can be their actual physical location or other locations connected to the provider of the data services.

HSBC wrote to Miss B and informed her that they weren't going to make any further refunds and were asking for the temporary credit back. They also informed her that her account was to be closed.

Miss B remained unhappy with how HSBC had handled her complaint and brought it to the Financial Ombudsman Service for an independent review where it was assigned to an investigator to look into.

Both parties were asked to provide information about the situation and Miss B was able to say that:

- She confirmed she'd been involved in an accident which had put her in a lengthy coma.
- Miss B provided details of her stay in hospital and a police report showing that an individual had been arrested for the theft. The report indicated that Miss B's phone and passport had been recovered, but not cards to several accounts.
- She'd approached the UK Embassy for help.
- She'd had to lodge her passport with the hospital due to a large bill that was unpaid.
- She'd suffered greatly from the incident and was left feeling with very dark thoughts about her own safety.

HSBC provided details of their investigation, which in summary showed:

- Three calls were made during the time Miss B said she was in a coma which they believed was her.
- IP address data shows consistent addresses both before and after Miss B said she was in a coma.
- The disputed transactions were made using both her card and genuine PIN and her mobile phone.
- There was no clear explanation how this information was compromised.
- Miss B's explanations for the security of her card and phone were inconsistent.
- Miss B said her ex-partner was with her at the time of the accident.
- The Apple Pay function wouldn't work without the phone being secured.
- The pattern of payments didn't follow any usual pattern following the theft of a card or a device.

After reviewing the evidence, the investigator didn't uphold Miss B's complaint. It was commented that:

- It was believed the calls were made by Miss B when she said she was in a coma.
- The details concerning the police report were confusing.
- Some of the dates surrounding the reporting were inconsistent.
- Miss B had told HSBC she lost several thousand from another account but told our service it was only £200.
- Inconsistencies surrounding WU transactions and whether Miss B held an account with them or not.
- The account activity didn't follow typical fraud patterns.
- There was a question concerning the source of some of Miss B's incoming payments which

were funding the disputed transactions.

- There were inconsistencies over the security implemented by Miss B for her phone and PIN.
- There were consistent IP addresses for both disputed and undisputed transactions and use of Miss B's device.

Miss B strongly disagreed with the investigator's recommendations and made further comments:

- That she was in hospital at the time, so couldn't have made the calls to HSBC.
- She hadn't read the police reports as they were in Spanish.
- The incoming payments into her account were from various business ventures.
- Some of the dates may have been estimated, but the incident caused such a traumatic affect, it's not reasonable to expect Miss B to have accurate recall.

As no agreement could be reached, the complaint has been passed to me for a decision. As part of my own investigation, I wanted to understand what had happened in more detail and asked Miss B for some further information:

- Miss B was able to provide details of medical bills for her stay in hospital and other evidence of her accident.
- Miss B didn't know why someone would impersonate her in calls with the bank.
- Evidence of her contact with the UK Embassy was provided.
- Miss B confirmed there was a disputed transaction on another account for about £35.
- Miss B confirmed her phone used Face ID (biometric protection) but the PIN could also be used which was easy to obtain in the country she was in.
- Her children were looked after by a nanny whilst she was in hospital and later collected by their father who took them out of the country.
- The accident had affected her memory.

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.

The relevant law surrounding authorisations are the Payment Service Regulations 2017 and the Consumer Credit Act 1974. The basic position is that HSBC can hold Miss B liable for the disputed payments if the evidence suggests that it's more likely than not that she made them or authorised them, but HSBC cannot say that the use of the card and PIN or the use of Apple Pay or internet banking conclusively proves that the payments were authorised.

Unless HSBC can show that consent has been given, it has no authority to make the payment or to debit Miss B's account and any such transaction must be regarded as unauthorised. To start with, I've seen the bank's technical evidence for the disputed

transactions. It shows that the transactions were authenticated using the payment tools issued to Miss B.

It's not my role to say exactly what happened, but to decide whether HSBC can reasonably hold Miss B liable for these transactions or not. In doing so, I'll be considering what is most likely on a balance of probabilities.

I've seen evidence provided by Miss B that shows she was involved in an accident whilst abroad. That evidence also shows she was in hospital for an extended time, during which the disputed transactions occurred. I've taken into account the impact this has had on her and have assessed the information against the difficult situation Miss B has found herself in.

Having said that, there are a number of inconsistencies with the information provided by Miss B with some of her answers given to the bank and our service.

The information provided by the police to Miss B concerning the report of theft shows that a local person was caught and found guilty of stealing her items, including her phone and passport. There's some confusion about who the letter was addressed to as Miss B referred to that person as the one who was involved in the theft (it's unlikely the police would be writing to them), but overall, the letter outlines what happened to Miss B's items, including the return of her phone and passport. I did note that the report recorded the theft was reported prior to Miss B waking from her coma.

Miss B said when she checked her account after waking from her coma, she used another phone (presumably because she hadn't had her original one back from the police). But, HSBC's audit of the use of her mobile banking shows only her original phone was used throughout this period. There was no other device added to her account, so it seems unlikely that Miss B could have registered another phone without the audit showing this.

HSBC referred to several calls they'd had in the time Miss B said she was in a coma. HSBC believed (as did our investigator) those calls were made by Miss B to obtain refunds on certain card payments made from her account. Miss B has said that she doesn't know why those calls were made, but they weren't made by her. On one call, details about a refund request for a payment (which was made prior to her accident) was discussed. The caller (who does sound like Miss B) knew enough information to pass HSBC's security and knew information about Miss B's circumstances to discuss payments and refunds. I haven't given too much weight to the assertion that the voices sound the same as this can sometimes be difficult to accurately assess unless specific voice matching security is used (I'm not aware that this was the case here). Whilst I accept that Miss B has provided documentation regarding her stay in hospital, it doesn't seem plausible to me that the person(s) who stole her phone (a local thief) would be able to obtain the relevant knowledge to convince HSBC they were the genuine account holder.

HSBC's records show that a number of conversations were held with Miss B where she told them that she'd kept her phone unlocked and that the personal identification number (PIN) for her card was written on a piece of paper kept in her purse. Later, Miss B also said someone could have seen her enter her PIN into an ATM. She later said that she hadn't recorded her PIN, but as it was her date of birth, it was easy to work out. Miss B has given a range of responses to the question of her PIN security, so it's been difficult to establish what the actual situation was. If Miss B had used her date of birth as her PIN, I'd have to consider if this was in line with the terms of her account which say not to use details that are easily guessed.

HSBC explained that a number of the disputed transactions were made using a payment function (Apple Pay) set up on Miss B's phone. Miss B had earlier said her phone was

unlocked but this function cannot be enabled unless basic phone security is switched on. So, it's unlikely Miss B's phone was unlocked and was likely enabled with biometric and PIN protection (which Miss B later said was the case). Miss B has said that it's possible to bypass the PIN on her phone in the country she was in – whilst I acknowledge her statement, I'm not convinced that's actually the case. There's no evidence to support that and it's difficult to see how her phone's own security was bypassed to enable the Apple Pay function to be used.

Miss B also told HSBC that her ex-partner was with her in the accident but was unhurt and he knew the PIN to her card. Miss B later told our service that her ex-partner wasn't with her, and she knew nothing of his whereabouts at the time of the accident. She also said the WU payments were linked to him. These are very different versions of what actually happened. Whilst I've taken Miss B's medical difficulties into account, I think these versions are so different that I can't be at all sure which explanation is the accurate one.

HSBC also referred to the use of Miss B's online banking (through her phone) which was accessed from common IP addresses and required security information known only to Miss B. This was used throughout the period Miss B says she was in a coma and HSBC argued that it was Miss B because a secure key was used to access the account. My understanding of the secure key is that it's (in this case) a separate device used to add additional authentication to certain transactions. Having reviewed this data there are a number of matching IP addresses from before both before the start of the disputed transactions and after (whilst Miss B was in hospital). So, I think it's reasonable to conclude that Miss B's phone was used by someone who had access to the same locations and the security key used by Miss B.

HSBC also didn't think the pattern of payments supported the assertion that it was a thief who'd stolen her details because the payments were for relatively low amounts made over a number of months. They didn't think they were in line with usual patterns of how stolen accounts are used. This isn't necessarily proof those payments were unauthorised. It's plausible here that whoever took Miss B's card(s) and phone also knew of her accident so could have known there was no rush to spend her money. So, in isolation, the pattern of payments isn't particularly useful in making a finding about authorisation. But, the statements do show that the account was used by someone who had regular access to it because the funds were generally spent when new (incoming) payments were made, avoiding overspending on the account.

One of the merchants (WU) responded to HSBC's enquiries and provided details of the payment(s) made through them from Miss B's account. This showed that two payments were made in Miss B's name to be collected in the same country she was in at the time (but whilst she was in hospital). The IP address used to arrange the payment matched one of those recorded by HSBC.

In summary, I do recognise the difficult circumstances Miss B has found herself in and I understand she will be disappointed with my decision, but I have to make it based on an objective review of the evidence. The inconsistent responses from Miss B have made it difficult to assess some of the evidence she's presented. There's little to explain how Miss B's phone came to be used by someone who could find the PIN and access it, find her online banking details, then knew enough about her personal situation to try and persuade HSBC that they should refund earlier payments, particularly given the details of those found guilty who appear to be local to the country Miss B was in at the time. I don't think it's plausible that a random thief would then start to request refunds from HSBC and be able to find someone who sounds like Miss B and knew enough to discuss the payments, at least one of which took place prior to the accident. The audit data shows the same device was used before, during and after Miss B was in hospital and no new devices were recorded.

I don't think the evidence supports that Miss B herself made some of these transactions she later disputed, but I do think, based on a balance of probabilities, that it's more likely than not that they couldn't have taken place without Miss B's knowledge or permission. It follows that I think it's both fair and reasonable that HSBC held her liable for the transactions she's disputed.

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 Miss B to accept or reject my decision before 28 October 2024.

David Perry
Ombudsman