<u>Ombudsman Decision</u>
<u>CIFO Reference Number: 25-000565</u>
<u>Complainant: Ms B</u>
<u>Respondent: HSBC Bank Plc, Jersey branch ("HSBC")</u>

The Complainant, who I shall refer to as Ms B, complains that HSBC should not have made a payment which she did not authorise and that it is refusing to refund it.

Background

On 20 October 2025 Ms B received a telephone call from someone claiming to be a member of HSBC's fraud team. He had tried to call several times, but Ms B was on holiday at the time and not well-placed to take calls. The individual said that a payment of €4,000 to an account in the UAE had been identified and that the bank wanted to check that it was genuine.

Ms B has explained that the individual asked her some security questions and, when she was unable to answer them correctly, said that the bank would send her a code, which she was then asked to provide to him over the phone. Ms B did that; she also said that she had not authorised a payment of €4,000.

The caller said he would lock Ms B's mobile banking app and told her not to log in to her account while he looked into things.

In fact, the caller was not from HSBC at all. Rather, he had been able to use the information which Ms B provided to register a new device on the account and then to transfer £88,000 – virtually everything in the account – to a different HSBC Jersey account.

Ms B was unaware that a new device had been registered on her account and did not know about the transfer. Having reflected on the conversation, however, she felt suspicious and called HSBC – around 20 to 30 minutes after the initial call. She made two calls, at 11:58 and 12:13 on 20 October 2025. Both were recorded, and the recordings have been provided to me. In both calls Ms B explained that she had received an unsolicited call from someone claiming to be from the bank's fraud department. She expressly asked whether there was any record of a security call having been made, as she had become concerned that the call may not have been genuine. On neither call did the agent answer that question. They did however discuss whether a €4,000 payment to UAE had been blocked. In fact, there was never any such payment or any attempt to make that payment.

Ms B assumed that everything had been resolved and that, if there had been an attempt to make a €4,000 payment from her account, it had been stopped.

It was not until around a week later that Ms B identified that a payment of £88,000 had been made from her account to a payee which I'll refer to as "T".

Ms B contacted HSBC, but it said there was nothing it could do to help. It refunded an overdraft fee because, combined with authorised payments made at around the same time, the unauthorised transfer had taken Ms B's account into overdraft. Through a representative, Ms B referred the matter to CIFO.

I considered what had happened. Having done so, I noted in correspondence with HSBC that Ms B had expressly asked about the call she had received apparently from the bank's fraud team. She had asked if such a call had been made but had not received an answer. I also said that I thought the £88,000 payment would have been apparent to the bank's agents when Ms B had spoken to them on 20 October 2025, but they had not mentioned it. Had they done so, I considered the fraud would have come to light almost immediately and action could have been taken to stop it.

HSBC said in response that it was satisfied it had followed the correct process and that it would not be offering reimbursement of Ms B's losses. It noted that Ms B did not mention the £88,000 payment when she called on 20 October 2025.

I invited the bank to reconsider its position. In doing so, I repeated that I thought its agents should have asked Ms B about the £88,000 payment. I also noted that it had not explained why it thought Ms B should be liable for a payment she had neither made nor authorised and of which she was unaware at the time.

Because no agreement has been reached on how Ms B's complaint should be resolved, I have reviewed the case file in full before reaching this Final Decision.

Findings

I have considered all the available evidence and arguments to decide what is, in my opinion, fair and reasonable in the individual circumstances of this complaint. Where necessary or appropriate, I reach my conclusions on the balance of probabilities; that is, what I consider is most likely to have happened, in light of the evidence that is available and the wider surrounding circumstances.

In line with my statutory duty to disclose evidence, I have provided copies of the documents which I have relied upon in reaching my decision.

Ms B's case is that she did not authorise the payment of £88,000 from her account to T. Rather, someone else was able to gain access to the account and then make the payment without her knowledge or authority.

HSBC has not challenged that point. That is, it has not suggested that Ms B's version of events is untrue or that she made the payment herself. Indeed, if that were the case, that would no doubt amount to fraud on Ms B's part. I am satisfied in any event that Ms B's account is accurate and true. It follows that she neither made the payment herself nor authorised someone else to make it.

I do think it likely however that Ms B provided the caller with sufficient information that he was able to register a new device to the account. He did that by persuading her that there was a risk the account had already been compromised. In fact, the attempted payment of €4,000 was a fiction designed to make Ms B think she needed to engage. The caller then invented security questions which were impossible to answer correctly. That gave him a reason to tell Ms B she would receive a security code. That code was a normal part of the log-in process and was sent by the bank to the mobile phone registered to the account – which, at that time, was still Ms B's.

Ms B was the only person authorised to operate the account. My starting point in cases such as this is that a bank cannot generally make payments from a customer's account without proper authority from an account holder or someone acting on their behalf (such as a holder of a power of attorney). It may be able to do so in exceptional circumstances (for example, under a court order or when exercising a right of set-off – neither of which applies here), or where the account terms allow it to do so.

As I have indicated, HSBC has not referred to any account terms which might, exceptionally, allow it to debit Ms B's account without her authorisation. Nor has it explained why, if there are any such terms, they might apply here.

As HSBC is aware, however, CIFO's general approach is that, if the account terms allow it to do so, a bank can only debit a customer's account in circumstances such as those in this case if it is able to show that the customer acted in a way which was "grossly negligent" – meaning that the customer demonstrated a very high degree of carelessness. I am not persuaded however that Ms B's actions met that threshold here.

Even if I were to take a different view on that point, however, I believe that the bank's handling of the two calls which Ms B made very shortly after she spoke to the fraudster is sufficient reason for reimbursement of the £88,000 payment.

It is in my view perfectly clear from the call recordings that Ms B was concerned she might have been targeted by fraudsters and that the earlier call might not have been genuine. The first call was around seven minutes long, and the second lasted around 26 minutes. Ms B expressly asked whether HSBC had called her about a payment of €4,000 to the UAE. She said she could not access her account. Her questions were not answered, even though the bank must have been able to check whether it had made an earlier call and whether any payments had been blocked.

Perhaps more significantly, no mention was made of the £88,000 payment to T. When Ms B made the second, longer call, that payment had either been made or was pending. Given the nature of Ms B's concerns and the reason for her call, I can see no good reason why the bank did not mention it. Simply as a matter of good practice, I believe one or other of the agents should have asked Ms B whether she had made it. Had that question been asked, Ms B would have said she had not.

I should comment that the bank has noted in its submissions that Ms B did not mention the payment in her calls on 20 October 2025. That, of course, is because she did not make it and did not know about it – having, as the bank knew, lost access to her account. Her call was not to report an unauthorised payment; it was to establish whether her account had been compromised and whether she had in fact been speaking to someone in its fraud department. HSBC was in a position at the very least to give Ms B information to help her establish whether that was the case, but it failed to do so.

The payment was, initially at least, made to another account with HSBC Jersey. I have asked the bank to provide information about any recall attempt. It has said that none was made, since Ms B did not report it as fraudulent until the following week, by which time funds would have been disbursed. (For reasons I have explained, Ms B did not know about the payment until around a week later.)

In my view, however, had HSBC alerted Ms B to the payment when she called to ask about the security of her account, it is likely that it would have been stopped or frozen – either before it had left her account or before it had left the account of the first recipient.

It follows that it would be fair for HSBC to reimburse Ms B for her losses.

In view of that finding, I do not need to consider whether, separately, HSBC's fraud detection systems should have identified the payment as fraudulent.

The details of HSBC's fraud alert systems are, of course, confidential. But most such systems will be triggered by a combination of factors, including but not limited to: the size of the payment; whether the payment is to a new payee; the method of payment; and the device used to make the payment.

In this case, the payment was substantial and amounted to virtually the entire balance on the account. It was to a new payee. It was made from a new device which had only recently been added to the account. And it was made at around the same time that the account holder had contacted the bank with concerns that her account might have been compromised. In short, it was in my view exactly the sort of payment that many people might expect to have triggered an alert. But, as I say and given my other conclusions, I don't need to make any finding on that point.

Final Decision

For these reasons, my final decision is that I uphold Ms B's complaint. To resolve it in full, HSBC Bank plc, Jersey Branch should pay Ms B:

– £88,000;

- Interest on £88,000 at 8% a year simple from 20 October 2025 until the date of payment; and
- £750 in recognition of the inconvenience Ms B has been put to and the distress caused by HSBC's actions.

Michael Ingram
Ombudsman

23 February 2026