DRN-5849347

## The complaint

Miss M complains that HSBC UK Bank Plc ('HSBC') declined to refund her £10,000 which she says she lost as a result of a scam.

## What happened

I wrote to both parties, sharing my provisional thoughts on this complaint in July 2025. The following is an extract from this provisional decision.

*"The details of this complaint are well-known to both parties, so I won't go into every detail of what happened here. But in summary, in February and March 2024, Miss M sent four payments from her HSBC account totalling £10,000. She sent the payments in order to help her sister secure a job and visa. Unfortunately, her sister had not been liaising with the relevant UK authorities as she had believed, and the funds were lost to a scammer.*

*Miss M was living and working in the UK, and her sister wanted the opportunity to do so too. Miss M's colleague gave her details of a company who may be able to help her sister find an employer who could sponsor her for a visa. When she contacted them they told her that they did not have any jobs going at the moment, but gave her the contact details of someone who may be able to help. Miss M got in touch with them via Whatapp, and they told her they were recruiting for care worker positions. She looked up the company online and found a professional and legitimate website which contained detailed information about the company. Her sister shared relevant documentation with them such as her identification documents, CV and relevant qualifications to help them find the most appropriate position for her. Miss M said her sister sent the 'company' applications for them to look over before she submitted them, too.*

*The company said that they required payment for their services and for assisting with the visa application. Miss M borrowed £10,000 to cover the costs. She sent two transfers, one on 21 February and one on 22 February, each for £2,675, to two individual's accounts. Then on 4 and 6 March she sent £2,500, then £2,150 to an account in her own name held with another business. She then sent the money from her other account to the scammers. HSBC did speak to Miss M when she was making the payment on 22 February. They asked her numerous questions about the payment, gave her a variety of scam warnings, and then checked if Miss M was happy to release the payment or if she wanted time to do any further checks on who she was paying or what she was paying for before she proceeded. Miss M said she was happy to make the payment, so HSBC released the payment.*

*When Miss M did not hear back from the company, she contacted them and they sent her and her sister an offer of employment. Miss M was confused as her sister had not been interviewed for this position, so she contacted the company through the email details on their website. The company emailed her back to tell her that they did not charge for their services and alerted her to the fact it was almost certainly a scam. Miss M reported it to HSBC, the other financial business she had an account with, and Action Fraud.*

*HSBC investigated Miss M's complaint and declined to refund any of her losses. In summary, they didn't think Miss M had established that she had met the requisite level of*

*care when she was making the payments to be entitled to a refund under the Contingent Reimbursement Model ('the CRM code'). They said they also contacted her to discuss concerns about the second payment and provided her with warnings which highlighted the risks and steps she should take to avoid being the victim of a scam. They also said that they had reached out to the recipient account businesses, who confirmed they were not liable in this case, and that no funds remained in the recipient accounts to return to Miss M.*

*Unhappy with their response, Miss M escalated her concerns to our service and one of our investigators looked into her complaint. They did not recommend that HSBC ought to reimburse Miss M's losses. In summary, they said that they thought there was enough going on for Miss M to have had concerns about the transactions she was about to make, and she should have taken further steps before making the payments. This meant under the code she had not met the requirements for her to be refunded. They said they did not think the payments represented such a scam risk that any further actions were required of HSBC.*

*Miss M did not agree. She said, through her representatives, that HSBC ought to have intervened on the first payment of £2,675 due to the stipulations of the CRM Code. They said that the code mandates that effective warnings ought to be provided and interventions where there are reasonable grounds to suspect a customer may be falling victim to a scam. She said that the payments were unusual and out of character for her account and ought to have triggered HSBC's fraud detection systems and provided a timely warning, potentially preventing subsequent payments and mitigating the financial loss. She said that this lack of intervention represents a failure in their duty of care. As no agreement could be reached, the case was passed to me to decide.*

*What I've provisionally 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. I am minded to reach the same overall conclusion as our investigator, and for broadly the same reasons. But, because I am presenting arguments which our investigator did not put forward in their original view of this complaint, it would not be fair to proceed to final decision without giving both parties the opportunity to respond to these new points with comments or evidence. But, if nothing changes, the following will likely be my final decision.*

*In broad terms, the starting position in law is that a bank is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Service Regulations and the terms and conditions of the customer's account. However, where the consumer made the payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the consumer even though they authorised the payment.*

*When thinking about what is fair and reasonable in this case, I have considered whether HSBC should reimburse some or all of the money Miss M lost in line with the provisions of the CRM Code it has agreed to adhere to and whether it ought to have done more to protect Miss M from the possibility of financial harm from fraud.*

*The CRM Code*

*HSBC was a signatory of the Lending Standards Board Contingent Reimbursement Model ('CRM') Code at the time of the transactions which required firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances. It sets out standards that banks, such as HSBC, are expected to meet in terms of protecting their customers from financial harm. But it also sets out expectations that a customer should meet, too. As a starting point, a customer should receive a full refund if*

*they fall victim to an authorised push payment scam such as this one. This does not include payments that customers make to an account held in their own name, so the two payments Miss M made to an account in her own name are not being considered under the CRM code here.*

*There appears to be no dispute that Miss M was the victim of an authorised push payment scam here. She thought she was sending money to help secure a job and a visa for her sister to join her in the UK, but instead it went to a scammer. But, Miss M would not be entitled to a full refund if HSBC can fairly and reasonably demonstrate, as they have asserted, that Miss M has failed to meet the requisite level of care under one of more of the listed exceptions set out in the CRM Code.*

*Those exceptions are:*

- *The customer ignored an effective warning in relation to the payment being made;*

- *The customer made the payment without a reasonable basis for believing that: the payee was the person the customer was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate.*

**There are further exceptions within the CRM Code, but they do not apply in this case.*

*Did Miss M have a reasonable basis for belief?*

*Unfortunately, I think the evidence suggests that Miss M did not have a reasonable basis for believing that she was dealing with a legitimate business when she made the transfers. I say this because:*

- *Miss M was asked to lie to her bank about the purpose of her payment. As Miss M thought she was dealing with a legitimate business who would be able to not only find employment for her sister, but help her secure a visa from UK authorities, it would seem highly unusual that they would ask Miss M to deliberately lie to her bank. If the payments were for legitimate purposes, it is not clear why a bank would decline to process them.*

- *I appreciate Miss M received the first phone number from a colleague who told her that they knew people who had used the business to gain employment and visas, but I think she could have done more due diligence on the second company before parting with this amount of money.*

- *Whilst Miss M looked up the genuine company that the scammer claimed to work for, she did not do any independent checks to make sure that the person she was talking to was in any way affiliated with the genuine company. It is clear from the circumstances in which the scam was discovered that a proportionate and simple check could have been to email the legitimate company's email, and this would have alerted her to the fact this was a scam before sending the funds. Whilst I appreciate some businesses will communicate with customers over Whatsapp, it is not a very official means of communication. So I'd have expected her to verify who she was speaking with before parting with funds.*

- *Miss M made the two transfers to named individuals. It is unclear why she thought that she needed to pay individual accounts when she believed she was paying a legitimate business. I have not seen that there was a reasonable explanation as to why she believed this was required, and would further the need to verify that she was*

*talking to the actual business before sending the money.*

- *Miss M did not seem to question what the funds were for beyond helping with securing work and visas. I have not seen evidence that she was given any kind of breakdown of fees and charges, or any kind of invoice. I'd expect a legitimate business to provide paperwork with requests for this much money.*

- *Further to this, Miss M sent the funds in full before her sister had even been offered an interview. I appreciate they provided some support in reviewing applications and asked for relevant documentation which would have made the business seem somewhat legitimate. But given the cumulative sums involved, and the lack of a breakdown of costs, it seems a lot of money to part with before any job or visa had been obtained.*

*Whilst some of these factors in and of themselves may not have persuaded Miss M not to make the payments, when considered collectively and considering the specific circumstances of this case and the factors in the round I think there were sufficient unusual factors here that Miss M ought to have acted more cautiously than she did.*

*I am satisfied, therefore, that Miss M did not have a reasonable basis for believing she was making a payment to a legitimate company, so HSBC are not required to give her a full refund under the CRM code.*

*Did Miss M ignore an effective warning in relation to the payment being made?*

*The code also sets out standards that banks are expected to meet, as I explained above. HSBC needs to be on the lookout for factors that might indicate an enhanced risk that Miss M's payment instructions were being made as part of a scam. Where they identify such a risk, the bank needs to take reasonable steps to provide the customer with an effective warning.*

*HSBC, in their submissions to this service, explained that the first payment did not require any warning to be given – and I agree. I don't consider the first payment of £2,675 was significantly out of the ordinary and therefore I do not think HSBC ought to have identified a scam risk. I appreciate this was not an inconsequential sum of money, but it was not sufficiently large or unusual such that it ought to have put the bank on notice. And so, I don't think HSBC needed to provide a warning for this payment.*

*It seems that HSBC thought that the second payment did represent a risk of fraud and financial harm to Miss M, as they paused the payment and spoke to her about it. So, I take this as HSBC accepting that this payment did require an effective warning. Miss M was provided with a series of in-app warning screens, before HSBC paused the payment and required her to speak with them. I've listened to this phone call and carefully considered whether HSBC met their required standard here.*

*They asked her why she was making the payment. Miss M was detailed in her cover story – saying that the person she was sending money to was a colleague who she knew well who was moving to Australia. She said she was going to buy their car, but by the time her loan came through, the car had been sold. She said her colleague was selling all of their furniture and homeware, and she decided to buy it to send it back to her family in a container (they live in another country).She said that it was the first time paying this person but that she had sent funds to the friend's mother the day before, and explained this was because the mother was travelling now. She said she got the payment details on WhatsApp but confirmed them verbally with her colleague for both sets of account details. She spoke about what sort of things she was buying now, and said she'd seen all of them and was happy with the quality*

*of goods.*

*For HSBC's part – they asked relevant and probing questions based on the information Miss M presented them with. They explained different types of scams and how they could unfold – including purchase scams and impersonation scams. They warned her of typical hallmarks of these different scam types and seemed to make sure that Miss M understood. Miss M assured them that no one was asking her to make payments on consecutive days, that no one had contacted her online or over the phone, that no one was on the phone with her at that time. HSBC also spoke of how persuasive scammers could be, and that they often impersonated genuine companies in order to deceive people. They warned Miss M of the consequences of proceeding with the payments if they later turned out to be scam payments – namely that it was likely she would not be able to get her money back. They asked if she wanted time to do any further checks before sending the funds, but she said she did not wish to, so HSBC released the payment.*

*Considering all of this, I think that HSBC's warnings were effective – they were timely, understandable, clear, impactful and specific to the types of scam risk identified during the call with Miss M. I think Miss M failed to act reasonably in response to the effective warning. And I think this failure to respond to the effective warning materially impacted the success of the scam. So, for the second payment, I think it is fair that this exception applies.*

*Is any refund due under the CRM code?*

*As I outlined above, the first payment did not require an intervention from HSBC and Miss M did not meet the requisite reasonable basis for belief that she was dealing with a legitimate business prior to making either of the payments. For the first payment, HSBC were not required to provide an effective warning, and for the second I am satisfied that they did and that it was ignored by Miss M. So, on this basis, I am not minded to ask HSBC to refund either of these payments as the relevant exceptions to reimbursement apply here. And I will not be asking them to refund the two payments to Miss M's own account under the code, as the code does not cover these payments.*

*Should HSBC have done any more to protect Miss M?*

*I've considered whether HSBC ought to have further intervened in the subsequent two payments. These payments went to her own account she held with another business, and were some time after the orignal two payments and for different amounts. I do not think there was anything about the subsequent payments ought to have alerted HSBC that Miss M was at risk of fraud or financial harm. They were made on separate days, to an account in her name which she had paid before, for different amounts and neither amount was of such a high value that it looked unusual or out of character. There had been previous payments of these kind of values. So I think it was fair and reasonable that HSBC did not intervene with these payments.*

*Recovery*

*I have also considered whether HSBC could have done more to try to recover the money once they had been told of the scam. I would expect a business to take reasonable steps to try and recover the money from the bank it was sent to. HSBC did try to recover the funds Miss M sent to the receiving bank – and were able to evidence that they had contacted the bank within a short amount of time. The receiving bank got in touch to say they had no remaining funds within the accounts. So, I don't think HSBC could have recovered Miss M's funds here.*

*My provisional decision*

*If nothing changes, I am likely to say that I do not uphold this complaint."*

**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.

Miss M's representatives got in touch to accept the provisional decision. HSBC did not have anything further to add. As nothing has changed, I will not be upholding this complaint for the reasons I explained in my provisional decision.

**My final decision**

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss M to accept or reject my decision before 28 October 2025.

Katherine Jones
**Ombudsman**