DRN-4327449

Complaint

Miss L is unhappy that HSBC UK Bank Plc didn't reimburse her in full after she fell victim to a safe account scam.

Background

In November 2021, Miss L received a text message which purported to be from HSBC. It asked her to confirm whether a particular card transaction had been made by her. She confirmed that it hadn't, and so she was called by someone claiming to be an employee of the HSBC fraud team. Unfortunately, this call was not from a legitimate employee of the bank, but a fraudster.

She was told that the security on her account had been compromised and that it was essential she move her money to a new 'safe account' which the bank had opened for her. She was also told that it was imperative that she not reveal to anyone (including any other employee of the bank) that she was being asked to do this. To do otherwise would risk tipping off the fraudster responsible for compromising the security of her accounts.

She made the following payments from her HSBC account:

27 November	£3,560 to Payee A
28 November	£6,100 to Payee B £3,200 to Payee B £4,200 to Payee B
30 November	£3,400 to Payee C £6,100 to Payee D
1 December	£6,800 to Payee D[1]

Each of the payments set out above was made to a named individual. She was told the first recipient was the name of the manager of her local branch of HSBC. She was told the subsequent three payments had to be made to a different person because the source of the funds was her savings account. They needed to be transferred to someone who dealt with that type of account.

HSBC temporarily paused the first payment on 27 November and spoke to Miss L before allowing it to go through. As instructed by the scammers, she told the HSBC employee that

[1] This payment was funded by the proceeds of a fraudulent loan application submitted in Miss L's name by the scammers.

the transfer was to pay for a kitchen renovation. The call handler gave a detailed explanation of the most commonly occurring scam types in order to warn Miss L about the risk that she too had been targeted by a scam. He said:

> *"There's a lot of scammers right now claiming to be from HSBC, from the fraud team or from the branch or even from other companies … who may send you an email, text message or even call you. So when these scammers call, they will tell you that the number you see on your caller ID is the same as the number on the back of your debit card … and also, these scammers will tell you that your account is already compromised and then they will tell you to transfer your money to people you do not know or to a fake account they pretend to open for you.*
>
> *Sometimes they will tell you they need your help with a fake investigation to catch a fake fraudster at an HSBC branch.*
>
> *[…]*
>
> *They will tell you to convince or mislead HSBC that the transfer is going to a builder, a family member, a friend, a safekeeping account or a loan for a family business."*

The HSBC employee then asked Miss L *"Have you received any calls, messages or emails similar to this?"* and Miss L said that she hadn't. She agreed to proceed with the payment. HSBC spoke to Miss L again in connection with the fourth transaction. The call handler asked her *"Is this a one-off transfer or will you be transferring more funds?"* Miss L said that there wouldn't be any more transfers. She said there were three separate invoices, and this was the final one. The next two payments were made without any queries from HSBC.

On 1 December, Miss L discovered that a fake loan application had been submitted in her name. She went to her local branch to explain what had happened and was told that a member of the fraud team would contact her later that day. She did receive a phone call, but it was from the fraudsters rather than HSBC. She was persuaded by the fraudsters to transfer the proceeds of that loan to Payee D.

Shortly afterwards, she visited the branch again and mentioned what had happened over the previous days. The branch staff recognised that she'd fallen victim to a scam. After an investigation, HSBC confirmed that it wouldn't refund her losses in full. It said that it had given her an effective warning on 27 November and that she hadn't done enough to verify the legitimacy of the call. However, it thought it should've given a warning in connection with payments 3 and 4 but didn't do so. As a result, it agreed to refund 50% of the money she'd lost when making those payments.

Miss L was unhappy with that response and so she referred the complaint to this service. It was looked at by an Investigator who didn't uphold it. She thought that Miss L hadn't taken sufficient care and that there were several red flags that ought to have put her on notice that the call was unlikely to be from HSBC.

Miss L disagreed with the Investigator's view. She said that HSBC should've done more to warn her about the risk of scams. She also argued that she was vulnerable at the time because she suffers with anxiety.

Because Miss L disagreed with the Investigator's view, the complaint was passed to me to consider.

Findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I issued a provisional decision on this complaint on 1 August. I wrote:

> *It's common ground that Miss L authorised the payments in question, albeit I accept that she was tricked into doing so. These were, therefore, authorised payments and so under the relevant rules and regulations, she is presumed liable at first instance. However, that isn't the end of the story. HSBC is a signatory to the Lending Standards Board's Contingent Reimbursement Model ("CRM") Code. The Code says that customers who fall victim to Authorised Push Payment ("APP") scams such as this one should be reimbursed, subject to some limited exceptions.*
>
> *One of those exceptions is that the firm can opt not to reimburse its customer if "the Customer made the payment without a reasonable basis for believing that … the person or business with whom they transacted was legitimate." I've carefully considered whether that exception applies here and, while I don't doubt that Miss L sincerely believed the request to be genuine, I'm not persuaded that belief was a reasonable one.*
>
> *As I understand it, the fraudsters didn't need to take any significant steps to persuade her that the request was genuine. They didn't have any information about Miss L or her accounts that one might only expect her bank to know. I also understand they didn't 'spoof' a genuine HSBC number – a commonly used tactic of fraudsters to persuade consumers that they are genuinely working for the bank. She seems to have taken the claim that this call was from HSBC at face value. I think she ought to have been more sceptical than she was, particularly when she was asked to make multiple payments to accounts belonging to named individuals without a particularly persuasive justification for doing so.*
>
> *I've also considered the information HSBC communicated to her about the fraud risk. The written warnings she saw when making the payments were not particularly relevant to the scenario she was faced with. On the instructions of the scammer, she'd selected a payment purpose that would display an irrelevant warning. However, HSBC spoke with Miss L in connection with the first payment. I've listened to that call and part of it is transcribed in the background section of this decision. The call handler gave her a detailed description of the potential scam types that might have been relevant in her circumstances. She was asked whether she'd received any messages or calls that matched the description she'd just been given and responded that she hadn't.*
>
> *I think this conversation was sufficiently detailed and relevant to the scam that she had been targeted by that it should've made her realise that this was unlikely to be a genuine request from an employee of the bank. For that reason, I'm satisfied that she made these payments without a reasonable basis for believing the request to be legitimate.*
>
> *Miss L also told the Investigator that she suffers with anxiety and takes medication prescribed by her doctor to help manage it. The CRM Code does apply differently where the customer is vulnerable. It says that a customer is vulnerable if "it would not be reasonable to expect that Customer to have protected themselves … against that particular APP scam." While I appreciate what Miss L has said about her mental health difficulties, I've not seen enough evidence to suggest that they meant she was*

unable to protect herself and so I'm not currently persuaded that she meets that definition.

Other considerations

In addition to its obligations under the Code, good industry practice required HSBC to be on the lookout for account activity or transactions that might be indicative of a fraud risk. In this instance, it intervened on the first payment Miss L made and didn't process it until it had asked her several fraud related questions and given her a verbal warning about the risks posed by commonly occurring scams. As I explained above, I'm satisfied that it did all that it could in connection with that first payment.

However, when Miss L spoke with HSBC the following day, she told the call handler that the fourth payment was the final payment she was making in connection with her kitchen renovation. She told the call handler that there would be no more payments and that there were three separate invoices she needed to settle.

In my view, it should've been concerned when further spending followed. She made a further payment to a new payee but also said that this payment was for a kitchen renovation. That contradicted what she'd told the HSBC agent in an earlier call and the introduction of a third payee suggested a strong possibility that the kitchen renovation was a cover story.

I think HSBC should, therefore, have paused the payment made on 30 November until it had spoken to Miss L to satisfy itself that she wasn't at risk of fraud. If it had done so, I think it's likely that the scam would've been uncovered. I say that because it appears that the coaching she was given by the scammer was superficial. I don't think it's likely she'd have been able to explain why further payments were required or who the new payee was. Essentially, I think if some straightforward questions about the transaction had been put to her, it's likely that holes in her cover story would've become apparent.

I've also considered whether Miss L can fairly be considered partially responsible for her losses. I've taken into account what the law says about contributory negligence but also kept in mind that I must reach a decision on this complaint based on what I consider to be fair and reasonable in all the circumstances.

Having done so, I'm satisfied that it's fair for Miss L to be considered partially responsible here. I've already made a finding that she made these payments without a reasonable basis of belief. I think that the 27 November phone call put her on notice that this request was unlikely to have genuinely come from HSBC and that she ought to have proceeded with greater caution. For the same reasons, I'm satisfied that it's fair and reasonable for HSBC to deduct 50% from the compensation it pays her.

Miss L disagreed with my provisional findings. In summary, she argued that:

- My findings were underpinned by personal opinion and that that shouldn't be a factor when reaching a decision on a case like this.

- She was in a state of panic and anxiety at the time she was dealing with the scammers. Her actions were reasonable ones if considered in that context.

- She disagreed with the finding I'd reached about whether she was vulnerable under the CRM Code. She pointed out that vulnerability is not necessarily a permanent

state and that she considers she was vulnerable at the time the scam took place. In support of that, she provided me with some background information about her personal circumstances, including the fact that she's a single parent on a low income and is responsible for caring for a child with significant learning difficulties.

HSBC also disagreed with my provisional findings. It responded to say that:

- Miss L misled HSBC on previous occasions so there was no reason to assume that she'd have responded differently if it had acted in connection with the final payment.

- She was clearly under the spell of the scammers and it is unlikely that she'd have acted differently. It suggested that she may have been coached by the scammers in case of further queries from the bank.

- It also disagreed that the payment was sufficiently out of character such that it would justify intervention.

I've carefully considered the further arguments made by both sides, but I'm not persuaded to depart from the position I set out in my provisional decision.

I want to be clear that I accept Miss L believed that the request to transfer her funds was a genuine one. However, my finding was that this belief was not a reasonable one for her to hold. It's not my intention for that finding to come across as judgemental – but the CRM Code includes a test that relates to the reasonableness of the customer's belief which I quoted in the provisional decision.

The Code can't prescribe every potential scenario and give guidance on which specific actions by a customer would be reasonable or not. It's my role to look at the available evidence and come to a determination based on what that evidence shows. It's inevitable, therefore, that my decision will use phrases such as *"I think"* – after all, the decision is setting out my thoughts on the matter. However, it isn't the case that my decision is based on a hunch, as she's said - I can assure Miss L I've thought very carefully about what the evidence shows.

I accept what Miss L has said about the state of mind she was operating in at the time. She was in a state of serious anxiety and panic and this had been induced by the scammer. However, the call she had with the bank on 27 November very clearly and directly addressed the scenario she was in. Miss L has queried the fact that I mentioned that the scammers didn't 'spoof' the HSBC number and that one wouldn't expect the average customer to recognise the number of their bank. Spoofing is a common trick used by fraudsters – to reassure a customer that the enquiry is a genuine one. They may call using what appears to be a number belonging to the bank and then ask the victim to verify it – for example, by looking up the customer services number online or checking the number on the back of their debit card. The fact that this doesn't appear to have happened in Miss L's case suggests that she took the claim that the call was from the bank at face value.

I agree with Miss L that vulnerability isn't necessarily a permanent state. I'm considering her complaint under the terms of the CRM Code. That Code defines vulnerability in the same way. Her personal circumstances at the time clearly were difficult. However, the Code requires that the customer's circumstances make it unreasonable to expect them to protect themselves. Lots of customers who find themselves in difficult personal circumstances can be more at risk of falling victim to a scam, but that doesn't necessarily mean that they meet that definition. I don't want to downplay the significance of the challenges Miss L has faced, but I'm afraid I don't find that they reach that bar.

In respect of the points raised by HSBC, I remain of the view that a further intervention was required. Miss L had told it that there would be no further spending – so the fact that spending restarted so soon afterwards, purported to be connected with the same payment purposes and was being made to a new payee – it was no longer credible to consider Miss L was making payments towards a kitchen.

I acknowledge the argument that she may simply have reiterated that the payments were for a kitchen, as she had done in the first call with the bank. However, by that point, I think HSBC ought to have assessed the later payment as being higher risk than the first one. Any intervention therefore needed to be proportionate to that risk. If she had been asked to account for why she was making further payments towards a kitchen renovation and to a third payee, I think it's unlikely that she'd have been able to give a compelling or persuasive explanation and the scam would therefore have likely come to light.

Final decision

For the reasons I've set out above, I uphold this complaint in part.

If Miss L accepts my decision, HSBC UK Bank Plc should refund her 50% of the £3,400 payment to Payee C and 50% of the £6,100 payment to Payee D. In total, that sum is £4,750. It should also add 8% simple interest per annum to that sum calculated to run from 30 November 2021 until the date it pays a settlement to Miss L.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss L to accept or reject my decision before 4 October 2023.

James Kimmitt
Ombudsman