DRN-5005728

The complaint

Mr K complains that HSBC UK Bank Plc won't refund the money he lost to a scam.

What happened

Mr K wanted to obtain a work visa which would enable him to remain in the country. He contacted someone who was a 'friend of a friend' who he'd been told could help him. He exchanged various messages with this person and, over a couple of weeks, made four payments to them for fees he believed were associated with obtaining this visa. Unbeknown to Mr K, he was speaking to a fraudster.

In total, Mr K paid £8,000 to an account controlled by the fraudster, from his HSBC account. But the visa never materialised, and the scammer stopped responding to him. Mr K reported the scam to HSBC in March 2024, around eight months after he had made the scam payments.

HSBC assessed Mr K's claim under the Contingent Reimbursement Model (CRM) Code, which it is a signatory of. The CRM Code sets out that HSBC should refund victims of authorised push payment (APP) scams (like Mr K), in all but a limited number of circumstances. HSBC said as Mr K didn't take enough steps to check who he was paying or what for, that he lacked a reasonable basis for belief. It also said that it felt it had provided Mr K with effective warnings regarding the first three payments he had made to the scam, so it declined to refund those payments to him. But HSBC did say it had not provided an effective warning for the last payment Mr K made, which was for £100, so it refunded that payment to him. HSBC was also unable to recover any funds from the bank account that Mr K sent his money to. Mr K was unhappy with HSBC's response to his complaint, so he referred his concerns to our service.

Our Investigator looked into Mr K's complaint, and they agreed Mr K didn't have a reasonable basis for belief under the CRM Code. They also felt that HSBC could not have done more to prevent the scam, so they did not feel it had failed in its obligations to Mr K under the CRM Code, they therefore did not feel that Mr K was entitled to a refund of any of his remaining loss.

Mr K did not accept this outcome, so as no agreement could be reached, this case was passed to me to be decided.

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.

It's not in dispute that Mr K made the payments to the fraudster himself. So, in accordance with the Payment Services Regulations 2017 he is presumed liable for the loss in the first instance. However, as I've already set out, HSBC is a signatory of the CRM Code.

The starting position under the CRM Code is that HSBC ought to refund Mr K, unless it can establish an exception to reimbursement applies. Such exceptions to reimbursement include (as far as is relevant to this complaint) that Mr K;

- 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

In this case, I think that HSBC has fairly established that the above exception applies. Overall, I find that Mr K ought to have done more to verify that the person he was dealing with was actually able to offer him what they claimed – a certificate of sponsorship and related visa. He appears to have received no paperwork, and he was arranging this all through an informal messenger service with an individual. The payments he made were also to that individual, not to any organisation that might be legally able to provide such services. And whilst I accept a recommendation from a friend might have been persuasive, it seems that Mr K knew very little about this individual, and given the large amount he was being asked to pay, and that there is freely available information online about the visa process and its associated costs, I think that Mr K ought to have had significant concerns about the transactions he was making. So, under the CRM Code, I think HSBC can fairly hold him at least partially liable.

Standards for firms

The CRM Code requires a firm to provide an effective warning where it identifies an APP scam risk in a payment journey. I'm persuaded there was enough going on for HSBC to have identified a scam risk when Mr K made the first payment of £3,000 given its value and that it was to a new payee. HSBC confirmed it did provide Mr K with a warning – about payments to 'friends and family' as that is the payment purpose Mr K selected – and I have seen the warning provided.

But I don't consider that warning meets the definition of an 'effective warning' as set out in the Code. While it does cover some of the hallmarks of relevant scams, it doesn't go into enough detail to really be effective. It doesn't highlight the key features of the scams it's designed to address clearly enough, so I don't think it can be considered as specific under the definition as set out in the Code.

However, the Code also says that the assessment of whether a firm has met the standard or not should involve consideration of whether compliance with that standard would have had a material effect on preventing the scam that took place. That is to say, had it provided an effective warning to Mr K, would that have prevented the scam?

But given that Mr K selected the 'friends and family' payment purpose, it's difficult to see how an effective warning provided by HSBC at that stage could have protected Mr K, as any warning would have been tailored to the payment purpose selected, which didn't reflect what Mr K was actually making the payment for.

It would, perhaps, have been more accurate for Mr K to have selected 'buying goods or services' as the payment purpose, but even if he had done this, I still don't think an effective warning would have brought this scam to light. As the fraud and scams landscape is ever evolving, it's important that firms continuously update their fraud detection systems to keep up to date with common scams. And purchase scams are well-known across industry and would certainly be considered a 'common' scam. But the specific variance of purchase scam in this case, that being the purchase of a visa, is not one which I'd consider to be 'common' at the time the payments were made, as it was not yet well-known across industry. I'm

therefore not persuaded it would have been reasonable to expect HSBC to have factored this specific type of purchase scam into its online warnings when Mr K made the payments.

I accept that during a conversation with Mr K, HSBC might have been able to uncover enough about what Mr K was doing to warn him that something didn't sound quite right. But this is not a case where I'd expect HSBC to have made direct contact with Mr K, such as via a phone call, to discuss things further. The payments he was making were not so high as to warrant such intervention, and were spread out over a longer period of time, rather than being made in quick succession. So, I consider that a proportionate intervention here would have been a written effective warning, but for the reasons I've explained, this would not have made a material difference to the success of the scam. And for these reasons, I find that HSBC is not liable for Mr K's loss.

Recovery of funds

HSBC says Mr K raised his scam claim in March 2024, eight months after the scam payment had been made, and it contacted the bank he sent the funds to at that time, but unfortunately none of Mr K's funds remained. And given the time that had passed since the scam payments, I can't see that there was anything more HSBC could have done here to recover Mr K's funds.

Whilst I'm very sorry Mr K has fallen victim to this cruel scam – and I have no doubt it's had a huge impact on his life both financially and emotionally, for the reasons I've explained, I don't find HSBC can fairly or reasonably be held liable for his loss.

My final decision

I do not uphold this complaint.

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

Sophie Mitchell
Ombudsman