DRN-5889213

The complaint

Mr K complains that HSBC UK Bank Plc has refused to reimburse money he lost to a scam

In bringing this complaint Mr K has been supported by a professional representative that I'll refer to as 'C'.

What happened

The background to this complaint is familiar to both parties and so I'll only refer to some key events here.

In February 2024, Mr K fell victim to a safe account scam, which led to him transferring £295,000 out of his HSBC account, which was subsequently lost to the scam.

Mr K explained he was contacted by someone purporting to be from his credit card provider's fraud department (which I'll refer to as 'A'). He said over the course of many hours of phone calls he was subjected to high-pressure tactics and manipulated into believing his credit card and bank accounts weren't safe and that he needed to transfer money to *"safe accounts"* to secure his funds.

Mr K made two payments - £25,000 and £250,000 on 20 and 21 February 2024 respectively - from his HSBC account to an account he held with an electronic money institution (which I'll refer to as 'R'). He then attempted a further £25,000 payment to an unknown third-party on 21 February 2024, but he later cancelled this instruction after HSBC asked him to complete the transaction in branch. On 23 February 2024 Mr K transferred £20,000 to another unknown third-party. Over the same period Mr K made more than 50 transactions from his account with R that were lost to the scam (which are the subject of another complaint that I will consider separately).

Mr K said he realised he'd been scammed when he was told by the scammer to visit a bank branch to meet with a fraud specialist but later discovered the person did not exist. At this point Mr K reported the scam to HSBC and asked it to reimburse his losses. HSBC refused. Mr K then complained that HSBC had failed to provide him with an effective warning that could have prevented his loss.

HSBC disagreed. It explained it had executed Mr K's payment instructions as requested and it did not consider he was entitled to reimbursement under the Contingent Reimbursement Model ('CRM') Code. It noted it had also intervened on each of his payments and warned him about safe account scams. It said that despite its warnings, Mr K had not been truthful when answering its questions and so had prevented it from uncovering the scam. It also said Mr K had not sought to protect himself from the scam, as he'd taken insufficient steps to confirm what he was being told was true. Unhappy with HSBC's response, Mr K referred his complaint to the Financial Ombudsman, with support from C.

Our Investigator didn't uphold the complaint. She explained why she was satisfied Mr K was not entitled to reimbursement under the CRM Code, in relation to the third-party payment. She didn't think Mr K had a reasonable basis for believing what he was doing was legitimate

and she was persuaded HSBC had met the standards for firms. She was also not persuaded that HSBC could reasonably have prevented Mr K's other losses, as he had given a cover story when he was asked by HSBC why he was making the payments, which prevented HSBC from uncovering the scam. He was also not responsive to scam warnings, even when they reflected what had happened to Mr K.

C disagreed on Mr K's behalf and asked for an Ombudsman's final decision. It said HSBC should have done more to verify what Mr K was saying, particularly in relation to the £250,000 payment he instructed in branch. While Mr K told HSBC he was transferring funds because he was moving abroad, C said HSBC's intervention should have gone further than it did and it ought to have requested tangible evidence to support what Mr K was saying. Had it done so, C suggested the scam could have been uncovered and Mr K's losses prevented.

The complaint has therefore been passed to me to decide.

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.

Having done so, I'm not upholding this complaint, and for largely the same reasons as our Investigator. I realise this will come as a disappointment to Mr K, not least because of the amount of money he has lost, but for the reasons I'll go on to explain I don't think HSBC has acted unreasonably in refusing to reimburse him in these circumstances.

When considering what is fair and reasonable, I'm required to take into account relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant time.

In broad terms, the starting position in law is that a payment service provider is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations (PSRs) and the terms and conditions of the customer's account. There is no dispute that Mr K authorised the payments – albeit he says he was tricked by scammers into believing they were going to 'safe accounts' to protect his funds, which was not true.

However, where a customer made payments because of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the customer even though they authorised the payment.

The CRM Code

As one of the scam payments Mr K made was an authorised push payment ('APP') to a third-party account held in the UK – the £20,000 payment on 23 February 2024 - the CRM Code is a relevant consideration.

HSBC was a signatory to the voluntary CRM Code, which provided additional protection to scam victims while it was in place. Under the CRM Code, the starting principle is that a firm should reimburse a customer who is the victim of an APP scam. But a firm can choose not to provide reimbursement if it can show that one of the exceptions to reimbursement apply, provided it also met the Standards for Firms.

So, I've considered whether any of the exceptions to reimbursement apply. I consider the most relevant exceptions in this case are R2(1):

a. *The Customer ignored Effective Warnings, given by a Firm in compliance with SF1(2), by failing to take appropriate action in response to such an Effective Warning given in any of the following:*

(iii) immediately before making the payment

(c) *In all the circumstances at the time of the payment, in particular the characteristics of the Customer and the complexity and sophistication of the APP scam, the Customer made the payment without a reasonable basis for believing that:*

i. *the payee was the person the Customer was expecting to pay;*

ii. *the payment was for genuine goods or services; and/or*

iii. *the person or business with whom they transacted was legitimate."*

Did Mr K have a reasonable basis for belief and did he ignore an effective warning?

I should note at this point that Mr K has been unable to provide much in the way of evidence to demonstrate what happened at the time of the scam. He has provided some explanation for this, as he said the scammers instructed him to delete messages and call logs, as part of steps to safeguard his account. I also accept that with scams of this nature there is often little in the way of documentary evidence to demonstrate what happened. So, I have accepted that events transpired as Mr K has described. I have also accepted that Mr K genuinely believed what he was being told at the time was legitimate. But the test I have to apply is whether or not he held a reasonable basis for believing this at the time.

In describing what happened, Mr K has said that on 20 February 2024, he received a call from someone purporting to be from A, advising him of an attempted transaction that would take him over his spending limit, and that his account and phone had been hacked. He was told he would receive another call from the bank that his credit card was linked with ('S'). Between 20 and 24 February 2024, Mr K said he was on the phone to the scammers throughout each day, for up to 13 hours at a time, and was being guided on what to do. He says he was also told:

- S was working with the Financial Conduct Authority ('FCA') to investigate the fraud;
- His account with HSBC was not safe and he needed to transfer his funds to an account he held with R, and from there on to other accounts held in third-party names;
- He needed to purchase crypto from a legitimate crypto exchange and then cash out those funds, which were paid into his R account and subsequently lost to the scam;
- That an HSBC employee was involved in the scam, which was being orchestrated by a larger criminal organisation, and so he should disguise the reason for his payments if asked by his bank;
- The people who had hacked his account knew his personal address, which presented a personal security risk to him and his family, but that the police had been informed.

Mr K says - although cannot evidence - that the original telephone call came from a number associated with A. He says he also received one-time passwords (OTP) from both S and the FCA, although he has only been able to evidence receiving an OTP that appeared to come

from the FCA on 23 February 2024, which was three days after he says the scam began. He says the phone number and the OTP reassured him what he was doing was legitimate, and I accept these factors added a veil of legitimacy to what he was being told.

But beyond this, Mr K took no steps to verify what he was being told – i.e. that there was a real threat to the safety of his accounts – or that who he was speaking with was legitimate. He has confirmed that he made no efforts to contact A, S, the FCA or the police to corroborate what he'd been told, despite the scam taking place over several days and involving the transfer of a considerable sum of money. He also doesn't appear to have questioned the overall plausibility of what he was being told, or how some of the steps he was being asked to take would help to safeguard his funds – for example why he needed to move funds from HSBC to R, before moving them on to a safe account, or why funds transferred to his crypto wallet weren't safe and needed to be moved again.

HSBC has also evidenced that it intervened before processing Mr K's £20,000 payment to the third party. It warned him that scammers had been known to impersonate HSBC and other financial institutions; had convinced customers there was fraud on their account; and persuaded them to move their money to a 'safe account'. It also warned that scammers had been known to coach their victims into not telling the truth about the purpose of the payment. Mr K was asked if he had received any calls like this. He said no. HSBC then asked Mr K about the purpose of his payment, but, on the guidance of the scammers, Mr K provided a cover story that the payment was a wedding gift for a family friend.

I consider HSBC's warning here would meet the standards, as set out in the CRM code, to be considered *"Effective"*. It was clear, impactful, timely and specific. I also consider Mr K ignored this warning, as he failed to provide HSBC with accurate answers in response to key questions asked that could have uncovered the scam.

Additionally, given HSBC's warning specifically highlighted the key factors that led to Mr K attempting to make the payment – i.e. a call warning about fraud on his account; an instruction to move money elsewhere and an instruction to lie to his bank, and having carried out no further independent checks to confirm what he was being told, I don't think Mr K could be said to have a reasonable basis for believing the payment was legitimate.

I'm therefore satisfied that HSBC could reasonably establish that an exception to reimbursement applied. I'm also satisfied that HSBC met the Standards for Firms as set out in the CRM Code, in terms of prevention, detection and response, having consider the steps it took to warn Mr K about scam risks, as well as its recovery attempts.

As such, I'm satisfied that HSBC was entitled to refuse to reimburse Mr K's loss in relation to the £20,000 payment under the CRM Code.

Should HSBC have otherwise prevented Mr K's loss?

Taking into account longstanding regulatory expectations and requirements, and what I consider to be good industry practice at the time, there are circumstances where it might be appropriate for HSBC to take additional steps or make additional checks before processing a payment to help protect customers from the possibility of financial harm from fraud.

The question then arises whether HSBC ought reasonably to have held such suspicions or concerns in relation to Mr K's payments - and if so, what might've been expected from a proportionate intervention at that time. Further to that, where there is an interaction between a customer and a bank before a high value payment is processed, as there was here, I'd expect the bank to take reasonable steps to understand the circumstances of that payment.

So, taking all of this into account, I need to decide if HSBC acted fairly and reasonably in its dealings with Mr K when he made the payments. Specifically, I have considered whether it should've done more than it did before processing them – and if it had, would that have made a difference.

But for me to find it fair and reasonable that HSBC should refund Mr K, I would need to find not only that it failed to intervene where it ought reasonably to have done so, or in the way it ought to have done - but crucially I'd need to find that but for this failure the subsequent loss would've been avoided.

That latter element concerns causation. A proportionate intervention will not always result in the prevention of a payment. And if I find it more likely than not that such a proportionate intervention by HSBC wouldn't have revealed the payments were part of a fraud or scam, then I couldn't fairly hold it liable for not having prevented them from being made.

HSBC did carry out checks before processing each of Mr K's payments. So, I have considered whether these were proportionate to the risk identified at the time, and if not whether proportionate intervention would most likely have prevented Mr K's loss.

Before processing the first £25,000 payment to his account with R on 20 February 2024, HSBC presented Mr K with an onscreen warning which said:

"Could this be fraud? […]

Is someone asking you to send money to a 'safe account'? If someone has told you to mislead us about the payment reasons or asked you to send money to a 'safe account', this is fraud. Stop now."

It intervened again, this time in branch, when Mr K instructed his £250,000 payment to R on 21 February 2024. Branch staff asked him about his transfer, and he explained he was moving abroad to set up a new business. He said he wanted to use his account with R because it offered better exchange rates than HSBC. From HSBC's records of this interaction, it seems branch staff provided Mr K with some generalised scam warnings, which included asking if anyone had contacted him and asked him to make the payment, but it did not give a specific safe account scam warning.

Considering the value of these payments and given Mr K's HSBC account had only recently been opened, I would have expected HSBC's intervention to have gone further than it did here. I would have expected it to ask further probing questions about how Mr K intended to use his funds. But unlike C, I do not think HSBC ought to have required Mr K to provide specific evidence to prove he planned to move abroad as he had said. While I would have expected HSBC to probe and challenge Mr K's answers, to test for any inconsistencies that may point to him being coached to provide a cover story, ultimately, I would have expected it to accept his answers on face value unless it had reason to doubt what he was saying. Here bank staff reported that Mr K was clear about how he intended to use the funds and his explanation for why he needed to transfer them to R seemed plausible.

While Mr K's answers in branch did not indicate he was falling victim to a scam, I think it would have been proportionate in the circumstances, to have provided him with more detailed scam warnings, including highlighting the risks of safe account scams, as it did in subsequent interventions. But ultimately, I'm not persuaded that, even if HSBC had intervened in this way, it would have led to the scam being uncovered or Mr K deciding not to proceed with the £250,000 payment, or any subsequent payment.

Throughout the duration of the scam, Mr K had multiple interactions with HSBC and R

regarding his payments. In each of these interactions he provided detailed cover stories for his payments. He was also repeatedly warned about safe account scams, which as I have set out above, highlighted the key hallmarks of this type of scam that ought to have resonated with him given the sequence of events he has described. Yet, despite these interventions Mr K chose to continue with the payments.

I'm mindful that Mr K has said that the scammers had manipulated him into providing the bank with cover stories for his payments, as he believed this was necessary to keep his funds safe. He was also led to believe that an HSBC employee may be involved in the scam, and so disclosing what was going on would put him at risk. But while I may understand Mr K's motivation for providing inaccurate information to HSBC (and R), I must nevertheless consider what impact this had on its ability to uncover the scam and ultimately protect Mr K from the risk of financial harm from fraud.

In light of the evidence, I'm not persuaded, on balance, that even if HSBC had intervened in the way I would have expected it to, this would have led to the scam being uncovered. I think Mr K would have continued to provide HSBC with answers that disguised the real reason for his payments, and I have no reason to believe any further safe account scam warnings would have resonated with Mr K, given his response to other clear and relevant warnings.

In the circumstances, I'm therefore unable to fairly conclude that proportionate intervention from HSBC would most likely have prevented Mr K's loss.

Could HSBC have done more to recover Mr K's losses

Lastly, I've considered if there was anything more HSBC ought to have done to recover Mr K's losses, but I don't think there was.

HSBC has evidenced that it attempted to recover the funds that were transferred to the third-party account when it was first notified of the scam, as it was required to under the CRM Code. Unfortunately, only £0.90 was recovered from that account, which has been returned to Mr K.

I would not have expected HSBC to attempt to recover any of the funds that were transferred to Mr K's own account with R, as this was within his control and therefore he already had access to any funds that remained.

In conclusion, I have a great deal of sympathy with Mr K being the victim of a scam which resulted in him losing a considerable sum of money. But it would only be fair for me to direct HSBC to refund his losses if I thought it was responsible for them, or if it was obliged to refund him under the CRM Code, but for the reasons I have explained above I'm not persuaded it was.

My final decision

For the reasons set out above, 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 15 December 2025.

Lisa De Noronha
Ombudsman