

The complaint

Mr N is unhappy that HSBC UK Bank Plc won't refund him money he lost as a result of falling victim to a fraud.

What happened

In October 2020, Mr N received an email purporting to be from the DVLA containing a link. Mr N clicked on the link and filled in the information requested. But he later realised that this may have not been legitimate and contacted HSBC to advise it of the circumstances.

Later, Mr N received a telephone call from someone purporting to be from HSBC's fraud department; Mr N says that the call displayed HSBC's official telephone number as written on the back of his bank card. The caller informed Mr N that a payment was attempted on his account and asked him to confirm if he'd carried it out. Mr N confirmed that he'd not. The caller then told Mr N that they'd call back and issue instructions on what to do next.

Mr N received the call back, as expected. The caller told Mr N that a payment had been set up on his account for £10,000 and this was due to be taken at midnight. The caller told Mr N that they'd set up another account where his money would be safe and that he should send the £10,000 to the 'safe account' via a trusted person's account. He was instructed that this should be done in two batches of £5,000 payments.

Mr N made a £10,000 payment to his partner's account and then, while the caller was on the phone, made the first of the two £5,000 payments from his partner's account to the 'safe account' details provided. After Mr N's partner made the initial £5,000 payment, Mr N became suspicious, contacted HSBC and uncovered the fraud.

HSBC looked into Mr N's claim but decided not to reimburse the £5,000 lost. It pointed out that Mr N had made the initial £10,000 payment to a trusted and legitimate payee, and therefore felt that the bank from which the funds were sent onto the fraudster should look into the claim instead.

Mr N disagreed and came to our service to look into his claim again. An Investigator considered the evidence provided by both parties and concluded that HSBC should reimburse the funds lost.

They pointed out that, while the payment was initially sent to a legitimate account, the payment was covered by the Contingent Reimbursement Model (CRM): a voluntary code signed up to by HSBC. When considering the complaint under this code, the Investigator found that Mr N was entitled to reimbursement of the money lost.

HSBC disagreed. It gave the following reasons why:

- The payment wasn't unusual as it was being sent to a trusted payee that Mr N had paid a number of times before. It would therefore have been difficult to identify the payment as a concern and prevent the scam.
- The CRM Code is not "*clear cut*" when dealing with multi-generational scams as the

code wasn't drafted with these in mind. It placed emphasis on some of the wording used in subsequent papers written by the CRM Code's author—the Lending Standards Board—highlighting that signatories to the code would not be liable in all cases involving multi-generation scams. It also pointed out that the account held by Mr N's partner was a signatory of the code and the Investigator's view didn't recognise the potential of shared liability.

- Mr N's acknowledgement of giving away personal information in a fraudulent phishing email, and the fact that he realised the suspicious nature of the call after the first payment, should have left Mr N more vigilant about the call.
- Mr N didn't sufficiently question the unusual nature of the instructions he was being given or verify the claims the caller was making about suspicious activity on his account.

As HSBC disagreed with the Investigator's view, the matter has now been passed to me to make a final decision.

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.

HSBC argues that the CRM Code should not apply to the payment Mr N sent to his partner. So, it does not believe Mr N is afforded the additional protection of the CRM Code and does not believe it is liable to reimburse him for the loss.

I have carefully reviewed the relevant material surrounding the scope of the CRM Code in relation to this type of scam. In particular, that includes the wording of the CRM Code, as it stood at the time in question, and the Lending Standards Board comments on the interpretation of that wording in its November 2021 publication: *'Call for Input: Findings Report'*.

In that report, the LSB describes "multigeneration APP scams" as follows:

"These scams, sometimes referred to as 'friends and family scams', typically involve a customer being duped into increasing the number of transactions and/or payees involved in the scam (for example, being convinced to transfer funds to a family member who in turn is asked to further forward them, onto the scammer's account). While the funds have been moved to a trusted third party, in that they are a friend or family member, the payment has left the control of the payee. This approach seeks to evade the detection and preventative measures of the Code [...]"

The report goes on to say that the investigation of such multi-generation scams *"is captured within the scope of the CRM Code"*.

The payment being disputed in the present complaint is one that Mr N made to his partner, under the misapprehension that he was acting under the legitimate instructions of his bank to secure his funds. I am satisfied that this payment meets the definition within the CRM Code of an APP scam – Mr N transferred these funds to another person for what he believed were legitimate purposes, but which were in fact fraudulent.

The loss here has been sustained by Mr N, and originated in the payment journey between Mr N's HSBC account and his partner's account. Mr N has suffered a financial loss through an APP scam, and a type of APP scam that the LSB says is captured within the scope of the CRM Code. His partner has not suffered a financial loss, and I don't consider that the use of her account as a conduit fundamentally changed the form of the APP scam that Mr N fell

victim to. I accept that the techniques used here by the scammer appear deliberately intended to evade HSBC's fraud detection and protection systems, but that does not in itself mean that the CRM Code ought not apply or that HSBC should not be liable.

HSBC argues that responsibility under the CRM Code should sit with, or partially with, the partner's bank and not with it. It directed Mr N to take up the loss he has suffered with his partner's bank. I do not agree.

Being the party that has suffered a financial loss here, Mr N reported the matter to HSBC. Receiving its customer's report of the scam, and in its capacity as the victim's bank, HSBC then has the principal responsibility for investigating and responding to the scam report (given this is the type of multi-generation scam caught within scope of the CRM Code). I consider that HSBC is also then responsible under the CRM Code for both the reimbursement decision and for reimbursement of the victim. Leading on from this the CRM Code goes on to state: *"Once a decision to reimburse has been made, the Firm of whom the APP scam victim is the Customer should administer the payment of the reimbursement to their Customer without delay."*

HSBC also has responsibility under the CRM Code to liaise with the other firms involved (that is not something the CRM Code requires Mr N, as HSBC's own customer, to do).

In short, I am satisfied that the CRM Code applies here, and that HSBC has the responsibility under the CRM Code to respond and, where appropriate, to reimburse Mr N. I consider that to be fair and reasonable in all the circumstances of this case.

On the basis that the CRM Code does apply to Mr N's transfer, I have therefore gone on to consider whether that means HSBC should have reimbursed Mr N for the loss.

Did Mr N fail to meet his requisite level of care under the CRM code?

I've first considered if Mr N failed to take the requisite level of care required for HSBC to choose not to reimburse him under the terms of the CRM Code: which it has agreed to adhere to.

The exception set out in the CRM code that is relevant to this case is:

- 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.

The CRM code also lists an exception whereby the customer ignored an effective warning in relation to the payment being made. But as no warning was given prior to the £10,000 payment being made, this isn't relevant to this complaint.

Did Mr N have a reasonable basis for believing the payment he made was legitimate?

HSBC have made a number of arguments that Mr N ought to have known he wasn't dealing with a legitimate request from his bank. I've outlined these arguments above in HSBC's response to the Investigator's view. However, I'm not persuaded HSBC has demonstrated Mr N didn't have a reasonable basis for belief, which permits it to refuse reimbursement under the code. I'll explain why.

Prior to receiving the call from the scammer, Mr N received an email purporting to be from the DVLA. Mr N clicked on a link within the email and provided personal information in the

website he was directed to. He later realised that this may have not been genuine and contacted HSBC to let it know.

HSBC has argued that Mr N's realisation that he'd likely given away personal information to an illegitimate source should have left him more vigilant to the call he later received from someone claiming to be from its fraud team. But I think Mr N did show vigilance in questioning the caller as to how he could be assured they were legitimate. He was asked to compare the telephone number he was receiving the call from against the number on the back of his bank card. And Mr N checked this and could see that it matched. I find it reasonable that this would have been a convincing tactic to gain his trust. Mr N has highlighted that he had no idea HSBC's number could be compromised which further shows this was a convincing factor in his basis for believing he was legitimately dealing with HSBC.

Furthermore, as Mr N was aware he may have shared personal details with an illegitimate source, and he'd passed this information onto HSBC, it wouldn't then be unreasonable for him to receive a call from HSBC's fraud department. I'm persuaded that the timeline of these events, along with the caller display showing HSBC's genuine number, would have provided a convincing deception.

HSBC has further argued that Mr N's realisation that he may have been scammed after transferring £5,000 of the £10,000 from his partner's account is further evidence that he knew the caller wasn't legitimate, but I don't agree. Fraudsters typically deploy high pressure tactics to skew their victim's judgement, and it's clear here that Mr N was concerned about his money being at risk. This no doubt would have impacted his ability to take a step back and evaluate the situation considering the urgency in which he was instructed to remove the funds that were at risk. I acknowledge that a request to move money from one account to another prior to sending it onto the 'safe account' is odd when looking at the circumstances with objective hindsight. But at the time, Mr N thought he was legitimately talking with his bank and therefore that he was following its instruction. He's also expressed to our service that personal circumstances meant that he was desperate not to lose his funds and he was acting swiftly to prevent this.

For the above reasons, I'm not persuaded that HSBC has been able to demonstrate that Mr N didn't have a reasonable basis for believing he was legitimately dealing with HSBC, and therefore failed to meet the requisite level of care. And so it follows that HSBC is unable to refuse reimbursement under the code.

Putting things right

HSBC should now go ahead and reimburse Mr N the £5,000 lost as a result of the fraud.

I agree with HSBC's submission that it would have been difficult for it to identify the payment as suspicious considering it was going to a trusted existing payee that Mr N had paid many times before. So, it should also pay 8% interest from the date it declined Mr N's claim to the date it settles, rather than from the date of payment as set out by the Investigator.

I've also considered the impact HSBC's error has had on Mr N. While I think it's important to acknowledge that the vast proportion of the impact caused was by the fraudster who has committed this callous crime, I'm persuaded that HSBC exacerbated this in its handling of the claim.

In addition to this, Mr N experienced a slight delay in having the remaining £5,000 reimbursed to him after it was returned from his partner's bank.

In recognition of this, I find that the £200 in compensation recommended by the Investigator

is fair in the circumstances to reflect the distress and inconvenience caused.

My final decision

For the reasons I've given above, I uphold this complaint and direct HSBC UK Bank Plc to:

- Reimburse Mr N the £5,000 lost
- Pay 8% simple annual interest on the amount lost from the date it declined the claim to the date of settlement
- Pay £200 in compensation for the distress and inconvenience caused

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr N to accept or reject my decision before 1 September 2022.

Stephen Westlake
Ombudsman