

The complaint

Mrs F complains that HSBC UK Bank Plc hasn't refunded her for payments she made when she was the victim of a romance scam.

What happened

Mrs F holds savings and current accounts with HBSC. On 18 June 2022, she says she met someone online on social media and started to message them. The person (who I'll refer to as M) said they were a US doctor currently working for the UN in Yemen. They began to exchange messages.

A few days later, M asked Mrs F for money. Mrs F says she initially sent a small sum. M then asked her for more. Mrs F says she was asked to pay several different individuals. None of the payments were being made to M, but Mrs F believed the payees worked with M and the money would be used to help M.

She received various documents from M, which reassured her he was genuine. It appears this included a marriage certificate dated 27 June, which was accompanied by several witness statements from people supposedly confirming they'd witnessed her marriage to M.

Between 26 June and 29 June, Mrs F made the following payments from her HSBC account:

Date	Payee	Payment Reason	Amount	Notes
26/06/2022	A	Paying for goods	£5,500	
26/06/2022	A	Family Support	£6,200	
26/06/2022	B	Family Support	£6,000	
27/06/2022	B	Family Support	[£10,000]	Payment blocked and reversed
27/06/2022	B	School fees	£5,000	
27/06/2022	A	School fees	£5,000	
28/06/2022	B	School fees	£5,000	
28/06/2022	B	School fees	£5,000	
28/06/2022	C	Buying goods	£6,000	
29/06/2022	Card payment		£4,000	
29/06/2022			[£2,000]	Blocked by HSBC.

TOTAL PAYMENTS SENT	£43,200	
---------------------	---------	--

Mrs F recalls that M had told her to hide the true purpose of the payments from her bank, which is why she'd chosen these payment reasons.

In addition to the payments from her HSBC account, Mrs F says she also purchased gift cards which she sent to other individuals, again with the intention of helping M.

By the point of the fourth payment from her HSBC account (the payment for £10,000 on 27 June) HSBC intervened. It blocked this payment instruction until it could speak to Mrs F.

Mrs F then called HSBC and it asked her various questions. Mrs F insisted that she wanted to make the payment. She denied anyone had influenced her to make the payment or that she'd received any messages telling her to make it. She said her father had asked her to make the payment to pay for medical treatment for her uncle. Her uncle was very sick and an old man. She said she'd made a payment to this payee before without trouble and insisted on the payment being released.

However, the phone line was poor quality – Mrs F explained she was travelling to London at the time. The call-handler didn't unblock her account. They told Mrs F that to unblock her account she'd need to visit a branch.

Mrs F visited a branch the next morning. She reiterated her cover story to explain why she had been making the payment – it was to support her family and help pay for medical treatment for her uncle. Mrs F again denied anyone had influenced her or coerced her into making the payment. But she said however that she now didn't need the payment to be made, she'd made alternative arrangements. It was cancelled for her.

On 29 June, HSBC blocked another payment attempt. When Mrs F spoke to the call-handler on this occasion, Mrs F immediately told the truth about why she was sending the money. The call-handler quickly identified it was a scam and prevented the payment.

HSBC then attempted to recover Mrs F's funds from the beneficiary accounts. It turned out that most of the money had already been moved on. However over £1,000 remained which has since been returned to Mrs F.

HSBC is a signatory of the Lending Standard Board's Contingent Reimbursement Model Code (the CRM Code) which can provide greater protection to the victims of Authorised Push Payment scams. All but the card payment on 29 June were push payment transfers and within the scope of the CRM Code. However, HSBC said it was not liable to refund Mrs F for these payments. HSBC said it had attempted to warn her when she was making the payments. It said she had made payments without knowing who she was paying or making any checks.

The bank explained that the card payment on 29 June wasn't covered by the CRM Code. It could have no valid grounds on which to chargeback that payment. Furthermore, it had no reason to have blocked the payment when Mrs F had authorised it. So overall, HSBC did not accept it was liable to refund either the bank transfers or the card payment made by Mrs F.

Mrs F didn't accept this outcome. She'd seen the warnings but says she was used to clicking past these without reading them, and therefore they'd had no impact on her at the time. She'd fully believed M was who he said he was.

Our Investigator considered Mrs F's complaint about HSBC. She sympathised with what had happened. But she didn't think HSBC had been at fault when it had reached the outcome it did. She thought that Mrs F had made these payments without having held a reasonable basis for believing the payments were going to whom Mrs F thought they were, or that they were for a genuine purpose.

The Investigator thought that even had HSBC provided more detailed scam warnings it would have made no difference – Mrs F would have most likely continued to insist on the payments being sent. Mrs F had deliberately deceived the bank about the payments and had done so without a good reason. HSBC didn't need to refund Mrs F.

Mrs F didn't agree. She thought the payments had been clearly out of character for her account. The bank should have realised this fitted the pattern of a romance scam. She'd not been given a detailed cover story so if the bank had asked further probing questions the scam would have been uncovered sooner.

In light of this disagreement, I have been asked to review Mrs F's complaint afresh and to reach a final decision on the matter.

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.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

Where the evidence is incomplete, missing or contradictory, I am required to make my findings based on a balance of probabilities – in other words what I consider is most likely given the information available to me.

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account.

These were 'authorised payments' even though Mrs F was the victim of a scam. Mrs F made the payments herself. So, although Mrs F did not intend the money to go to a fraudster, under the Payment Services Regulations 2017, and the terms and conditions of her account, Mrs F is presumed liable for the loss in the first instance.

As noted above, the CRM Code can provide additional protection, including reimbursement in some circumstances, where bank transfers were made as part of an APP Scam. However, it does not mean that a bank will always need to reimburse its customer. Even where payments are covered by the CRM Code, a bank need not fully reimburse the loss where it can establish the customer made the payment(s) without holding a reasonable basis for believing what they did.

Relevant here, that includes the basis for believing the payment was being sent to the person the customer thought they were paying and for genuine goods or services. Here, HSBC and the Investigator both concluded that Mrs F didn't have such a reasonable basis of belief.

I've considered the evidence available to me to decide whether I agree, and so whether that point has been correctly established by HSBC.

I understand Mrs F's point that she had believed M was who he said he was. But there were a number of features here that I think should have caused her to pause and question what was really happening.

It appears M first requested money from Mrs F not long after they first began exchanging messages – within a few days only. The reasons Mrs F was given for these payments aren't completely clear, nor is it clear why she needed to pay these individuals (rather than M for instance).

Mrs F says M led her to believe the money was needed urgently. But it's unclear what the reason for this was.

Nor is it clear why Mrs F was required to lie to her bank about the payments. I accept that in some limited circumstances, or in some specific types of scam, a customer might reasonably believe the right thing to do is to disguise the true purpose of a payment. But in the circumstances of this complaint, it seems unclear why Mrs F thought she needed to do this.

She believed she was in a relationship with M and was simply sending money to help him. In those circumstances she did not need to deceive her bank when the bank took steps to try to protect her. Being presumably prompted to do by M should have been a significant warning flag.

During the course of the scam, M sent Mrs F a falsified marriage certificate accompanied by fake witness statements. I've seen nothing to lead me to believe that Mrs F couldn't or wouldn't have realised that she could not have genuinely been married in her absence, or that UN employees could not have genuinely signed these witness statements. I think reasonably, Mrs F would have known this was false. Furthermore, this fake marriage ceremony was purported to have taken place just over one week after she'd first made contact with M, and without her having met him in person.

In short, I find there were enough points of concern here that Mrs F ought to have had serious doubts about the legitimacy of what M was asking her to do and the payments she was being asked to make.

In saying this, I accept Mrs F had been deceived by M into believing he was who he said he was and that the money she would send was to be used for his help. But taking everything into consideration, in particular those factors I've listed, I find that HSBC has been able to establish that when Mrs F made these payments, she did so without holding a reasonable basis for what she believed.

Where someone was vulnerable to a scam at the relevant time(s), the CRM Code would nevertheless provide for them to be reimbursed, even where they made the payment without a reasonable basis for believing what they did. For this purpose, the CRM Code defines vulnerability as being circumstances where it would not be reasonable to expect that customer to have protected themselves.

None of the parties have provided evidence to show that Mrs F would meet that definition. I've seen nothing else to make me think it should apply here. I don't find HSBC is liable to refund Mrs F through the vulnerability provisions of the CRM Code.

I've gone on to consider whether HSBC is otherwise liable to reimburse Mrs F under the CRM Code - for example through a failure to meet the standards set by the code that was

material to the success of the scam.

I've therefore listened to the available call recordings and considered the in-app warning messages shown to Mrs F.

Of course, in part, HSBC was hindered in its endeavours to protect Mrs F by her deception about the true purposes of the payments. That included the information she'd input into her mobile banking app as well as what she later discussed with HSBC verbally on more than one occasion. Despite this, some of the warnings given did relate to the appropriate scam type.

Overall, I'm satisfied that HSBC did attempt to provide Effective Warnings to Mrs F (as required by the CRM Code). Having said that I don't consider these warnings met the minimum requirements under the code. That is perhaps unsurprising given that the bank was being deceived about the true nature of the payments. Specifically though, I don't consider the warning messages were sufficiently impactful.

However, that isn't sufficient in itself to cause HSBC to be liable to refund under the terms of the code. A failure to provide an Effective Warning needs to have had a material effect on the success of the scam, and I simply don't think that applies in the specific circumstances of this case.

When HSBC did intervene, the evidence from the time leads me to believe that Mrs F was determined to disguise the true purpose behind the transfers. It seems to me that she was consistent in her denial of anyone having influenced her to make a payment or telling her to deceive her bank about it. While she says she wasn't given a detailed cover story, it does seem that she stuck to a consistent explanation, and one which wasn't obviously false.

In these circumstances, I'm not persuaded that even an Effective Warning would have caused Mrs F to not make the payments she did. Indeed, when she encountered difficulties in making the fourth payment, she tried again the following day for a smaller sum – it didn't prompt her to question what she was doing. So, all considered, I don't find there was a material failure by HSBC in relation to the protection standards set by the CRM Code.

Similarly, it's not apparent to me that further questioning would necessarily have led to the scam's earlier detection or prevention. Of course, it immediately came to light when Mrs F voluntarily revealed the truth to HSBC - but I find her earlier dishonesty had significantly impeded the bank in its efforts to identify the true situation sooner. Based on what I've seen, I don't find the bank was at fault in believing what Mrs F told it when it questioned her.

I've given additional consideration to the single payment made by card (the one payment here that is not covered by the CRM Code). The payment was made to a valid merchant, and it appears that the merchant provided the service paid for (the transfer of funds to a beneficiary). In those circumstances it seems to me unlikely there could be any valid chargeback claim available. Further, the transaction was correctly authorised by Mrs F, and even had HSBC found reason to contact her about it, I'm not persuaded this would have resulted in a different outcome. I've seen nothing to suggest this would have resulted in a materially different discussion than took place in relation to the earlier bank transfer payment.

When the scam was ultimately uncovered, HSBC could have notified all of the beneficiary banks faster than it did. But unfortunately, almost all of Mrs F's funds had already been moved on from the beneficiary accounts. That meant very little remained for HSBC to recover and return to Mrs F. What remained at the point Mrs F first reported the scam to HSBC has now been returned to her. I don't require HSBC to do more.

In summary then, I don't find HSBC was wrong to deny reimbursement under the CRM Code, and I don't find it liable to refund for any other reason.

That is not to take away from the fact that Mrs F has been the innocent victim of a criminal scam here. I have natural sympathy for her, especially in light of the impact she describes this having had on her. However, that impact principally resulted from the actions of the scammers who deceived Mrs F. So that does not, in itself, make HSBC liable for her financial losses. As set out above, I do not find HSBC needs to reimburse those losses and does not need to do more than it has already done.

My final decision

For the reasons given above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs F to accept or reject my decision before 25 April 2024.

Stephen Dickie
Ombudsman