DRN-4341990

## The complaint

Mrs G complains that HSBC UK Bank Plc won't reimburse her the money she transferred to a fraudster.

## What happened

Mrs G and her family were planning to make a holy pilgrimage to India and were looking to book both flights and a hotel for the journey. Mrs G's father was given the details of a particular travel website to book through from a senior family at their temple and so, on this recommendation, Mrs G's father booked his trip with an individual he believed to be an agent of this website. Unfortunately, unbeknownst to Mrs G's father at the time, the individual he was corresponding with was in fact a scammer.

Mrs G's father received confirmation of his flight, which he was able to verify on the flight company's direct website. Mrs G's father was told by the agent that he could also arrange travel for the rest of his family. On this basis, Mrs G and other members of her family decided to book through the same 'agent'.

Before making any payments, Mrs G has explained she checked the travel company website and was reassured that it seemed secure, based in the UK and that the company had been active for a long period of time. She was also reassured that the recommendation for the website had been provided by a senior family at the temple, and that her father had successfully booked his trip.

When booking the remaining family member's flights, the fraudster said that the only payment method he accepted was bank transfer - and that he also only accepted payments to be made from one specific banking provider (not HSBC). The majority of payments to the fraudster were therefore made by another member of Mrs G's family, who owned an account with this specific banking provider requested. However for the final payment, the fraudster advised that the agency's bank account was full and therefore the final payment due of £950 needed to be made to a different beneficiary account. This payment was therefore made by Mrs G by faster payment from her HSBC account. Mrs G was told by the fraudster to select 'friends and family' as the reason for payment, otherwise the payment wouldn't be accepted. He said this ensures you are keeping a record for your own purpose and not the bank's.

Mrs G and her family largely communicated with the fraudster using instant online messaging, but also via phone and email. Mrs G has explained that when sending voice messages via instant messaging, the fraudster insisted on speaking in Urdu, although otherwise communicated in English. Mrs G has provided copies of the emails sent by the fraudster, which shows he used an email address mimicking the name of the website he purported to be working for. His email signature also referred to flights being ABTA and ATOL protected which reassured Mrs G.

After making the payment to the fraudster, Mrs G has explained she received no follow-up confirmation emails. She's explained she also contacted the hotel she believed she was booked with, but they could not locate a booking in her name. Mrs G therefore tried to contact the fraudster multiple times, but her calls were ignored. When Mrs G's call was eventually answered, she said the fraudster told her she had been scammed and wouldn't be getting her money back. Mrs G's family also found that her father's booking had been cancelled. Mrs G therefore contacted HSBC to report she'd been the victim of a scam.

HSBC investigated Mrs G's fraud claim and considered its obligations to provide Mrs G with a refund. HSBC is a signatory of the Lending Standards Board Contingent Reimbursement Model (CRM) Code which requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances. HSBC says one or more of those exceptions applies in this case.

HSBC has said Mrs G didn't have a reasonable basis for believing she was making a genuine payment. HSBC considers Mrs G ought to have done more checks to make sure the person she was making the payment to was genuine.

It also contacted the beneficiary bank to attempt to recover Mrs G's money, but unfortunately no funds remained in the account.

Mrs G disagreed with HSBC so brought the complaint to our service. One of our investigators considered the case and didn't uphold it – she thought that, in the circumstances, Mrs G ought to have completed further checks to verify that she was dealing with a genuine company. The investigator therefore didn't consider that HSBC needed to do anything to put things right for Mrs G.

Mrs G didn't agree with the investigator, so the case has been referred to me for a 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.

Having done so, while I'm sorry to disappoint Mrs G, I'm not upholding her complaint. I'll explain why.

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.

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

When thinking about what is fair and reasonable in this case, I've considered whether HSBC should have reimbursed Mrs G under the provisions of the CRM Code and whether it ought to have done more to protect Mrs G from the possibility of financial harm from fraud.

There's no dispute here that Mrs G was tricked into making the payment. She thought she was making a genuine payment to a travel website and that didn't happen. But this isn't enough, in and of itself, for Mrs G to receive a refund under the CRM Code. The Code places a level of care on Mrs G too.

*The CRM Code*

As I've mentioned, HSBC is a signatory of the Lending Standards Board Contingent Reimbursement Model (the CRM Code) which requires firms to reimburse customers who have been the victims of Authorised Push Payment (APP) scams like this, in all but a limited number of circumstances and it is for HSBC to establish that a customer failed to meet one of the listed exceptions set out in the CRM Code.

Under the CRM Code, a bank may choose not to reimburse a customer if it can establish that*:

- The customer ignored what the CRM Code refers to as an "Effective Warning" by failing to take appropriate action in response to such an effective warning
- The customer made payments without having 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

**Further exceptions outlined in the CRM Code do not apply to this case.*

I think HSBC has been able to establish that it may choose not to fully reimburse Mrs G under the terms of the CRM Code. I'm persuaded one of the listed exceptions to reimbursement under the provisions of the CRM Code applies.

Taking into account all of the circumstances of this case, including the characteristics of the customer and the complexity of the scam, I think the concerns HSBC has raised about the legitimacy of the transaction Mrs G was making are enough to support its position that she didn't have a reasonable basis for believing the person she transacted with was legitimate. I'll explain why.

I appreciate that, prior to making a payment to the fraudster, Mrs G had received a recommendation to use the website in question to book her trip from someone she trusted and respected – and I don't doubt this would have strongly influenced her decision to trust that the individual she was paying was genuine. I also understand that she would've been strongly reassured by her father's apparent successful booking with the agent.

However, I also think that by the time Mrs G made the payment to the fraudster herself, there were a number of red flags that ought to have caused Mrs G to question the legitimacy of the individual she was making a payment to.

Having considered all the available evidence, I think it's most likely that the website Mrs G's family were recommended is in fact a genuine comparison site but that unfortunately, Mrs G's family were corresponding with an individual that was only purporting to work for that site. I say this because, having reviewed the website in question, it clearly states that it is a search engine that provides flight and hotel deals available in the market. It also states it is not a travel agency and does not sell flight tickets or holiday packages but directs customers to approved travel partners for booking completion. Mrs G has advised she was aware of this but believed the agent she was speaking to was booking flights on behalf of other agents. However, based on the website's own explanation of its services, I think it's reasonable to question why customers would be paying a search engine site directly and how the fraudster's role as an 'agent' fits into this service.

I also think the method of payment requested by the fraudster should have raised concern for Mrs G. The fraudster initially told Mrs G and her family it would only accept payment from one specific banking provider, which I think would be an unrealistic request from a genuine company. This request was also undermined when Mrs G then was able to make the final payment through her HSBC account. I also think Mrs G ought to have had cause for concern when the fraudster specified that payments should be made under the 'friends and family' payment purpose, particularly when this was clearly not the case. I think the reasons

provided by the fraudster for insisting payments were made in this way were questionable and not what would be expected from a legitimate firm. Lastly, I don't think it was realistic for the fraudster to state that the first bank account Mrs G's family made payment to was 'full' and this ought to have been questioned further by Mrs G before making payment to an account in an individual's name which appeared unrelated to the company, or anyone her family had been liaising with.

I appreciate Mrs G had confidence in the individual she was speaking to as the website she'd reviewed led her to believe she was in contact with a UK based company. However, having reviewed the website further I can see that the part of the website Mrs G is referring to is where you select your own country of residence. The website does state it's registered in Denmark and the email address provided on the site has a different domain name to that Mrs G was corresponding with (albeit similar). There are also no contact numbers listed on the site, so it's not clear where Mrs G's family obtained the phone numbers or email addresses from that they were using to liaise with the fraudster. However, there are no direct links between these contact details and the website Mrs G believed they were linked to.

I also think that, as Mrs G believed she was dealing with a UK based company, it ought to have been a cause for concern that the fraudster insisted on corresponding at times in Urdu – and that this ought to have been questioned further before proceeding to make payment.

With all of the above in mind, in the particular circumstances of this case, I consider that Mrs G ought to have had concerns about the legitimacy of the company she believed she was making payment to and that, in turn, ought to have led to a greater degree of checking on Mrs G's part. In not carrying out sufficient checks I don't find she had a reasonable basis for believing she was dealing with a genuine travel agent and so fell below the level of care expected of her under the CRM Code.

*Should HSBC have done more to try to prevent the scam and protect Mrs G?*

I've thought about whether HSBC did enough to protect Mrs G from financial harm.

The CRM Code says that where firms identify APP scam risks in a payment journey, they should provide Effective Warnings to their customers. The Code also says that the assessment of whether a firm has met a standard or not should involve consideration of whether compliance with that standard would have had a material effect on preventing the scam.

I am also mindful that when Mrs G made this payment, HSBC should fairly and reasonably also have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things).

Having considered the payment Mrs G made, I don't think it was so remarkable, in comparison to her usual account activity, that it should've appeared as suspicious to HSBC. I therefore don't think HSBC failed to meet its standards under the Code by not providing Mrs G with an effective warning, prior to processing the payment.

Once it was made aware of the scam, HSBC tried to recover Mrs G's funds, but unfortunately was advised by the beneficiary account that no funds remained. I don't think HSBC could reasonably have done anything further to recover Mrs G's payments.

Overall, I'm satisfied that HSBC's position on Mrs G's fraud claim, and its assessment under the CRM Code, is fair and reasonable in all of the circumstances and that HSBC shouldn't be held liable for Mrs G's losses. And so I don't intend to make an award to Mrs G.

I do sympathise with Mrs G as she's clearly been the victim of a cruel scam. And I don't doubt Mrs G genuinely believed she was speaking to a travel firm. But the circumstances of the case and the evidence available lead me to find I'm unable to uphold this complaint.

## My final decision

For the reasons I've explained, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs G to accept or reject my decision before 14 February 2024.

Kirsty Upton
**Ombudsman**