DRN-4608405

Financial Ombudsman Service

The complaint

Mrs H complains that HSBC UK Bank Plc trading as first direct won't reimburse her after she fell victim to a scam.

What happened

Mrs H has explained that in September 2023, she received a phishing email, appearing to come from Royal Mail, requesting for her to pay a small additional postage fee for a parcel she had been sent.

Not realising the email was a scam, Mrs H provided her bank card information, as well as personal information such as her phone number. Upon speaking with family members, Mrs H realised that she had provided her account details to fraudsters and contacted first direct to place a block on her card. While on the phone to first direct, the phone advisor told Mrs H that often, fraudsters won't attempt to make payments immediately, but will call victims pretending to be from their bank and advised Mrs H to watch out for these calls. After taking further information from Mrs H, the advisor read a script to Mrs H that included the following information:

'Fraudsters contact people unexpectedly and they send texts or emails pretending to be from companies or organisations we trust, such as Royal Mail, the NHS, the Police, banks including first direct and many more. Once the fraudster has your details they'll call you pretending to be from your bank, they might not call you straight away, it could be days or weeks after your details have been compromised and they will be very convincing. It is very likely that you will be contacted by someone pretending to be us. I would probably suggest if you do get any phone calls, just end the call and call us back on a different phone and if it was us, we can obviously pass you through to whoever it was.'

The advisor also told Mrs H that fraudsters may tell her to send her money to a safe account.

The following day, Mrs H received a call from a withheld number from another fraudster purporting to work for the Financial Conduct Authority (FCA). He told Mrs H that as a result of her providing information the previous day in a phishing email, they had identified a fraudster attempting to remove funds from Mrs H's account. Mrs H was advised that direct debit set-ups had been attempted, a loan had been attempted to be taken out in her name and that the Royal Mail falsified charge she had made had been amended to a much higher figure. Mrs H was therefore led to believe her funds were in danger and she needed to move her money to a safe account.

Mrs H has acknowledged that she did initially have suspicions about the caller and asked how she can be sure it wasn't a scam. The fraudster sent Mrs H a text message, the sender appearing on Mrs H's phone as 'FCA'. The text included a code and advised Mrs H that this code could be used to confirm the identity of the advisor. The fraudster then told Mrs H the code included within the text, which reassured Mrs H that the call was genuine.

Mrs H transferred her funds from her savings (£20,000) to her current account, then transferred these onwards to the account details provided by the fraudster, which Mrs H was told was the account of one of the FCA's colleagues. Mrs H was given a scenario to provide to her bank should they ask - that the funds in question were to purchase a car.

When making the payment transfer, Mrs H passed through first direct's fraud detection warning systems. Mrs H was advised by the fraudsters to select 'friends and family' as the payment purpose.

As a result, Mrs H was provided with the following warning:

'Caution – this could be a scam

WARNING** – If someone has told you to mislead us about the reason for your payments and/or choose the wrong payment type, **stop, this is a scam.'

The warning then went on to provide information about scams relating to friends or family scenarios, such as dating and social media scams. Mrs H has explained the fraudster told her to just click through these warnings as they were part of first direct's standard processes, which resonated with Mrs H as she explained they had appeared previously when making payments.

Following this payment transfer, Mrs H was told by the fraudster that the FCA thought the fraudster may be an internal employee of first direct. Mrs H was therefore asked to take out a loan with first direct and transfer this to another FCA 'colleague'. Mrs H was told that the bank's actions would indicate their involvement. Mrs H took out a loan for £15,000 and attempted to transfer £10,000 to another new payee. This payment was stopped by first direct and Mrs H was directed to contact her bank.

The fraudster told Mrs H to stick to a scenario it had provided her with, so as to not impact its investigation into first direct. Mrs H called first direct and explained she needed to make a payment to someone urgently today. First direct asked Mrs H about the loan she had taken out. Mrs H advised first direct (incorrectly) that the loan was for £10,000, which first direct questioned her on further, as well as the prior £20,000 payment she'd made that day.

First direct then asked Mrs H whether she had been coached on how to answer its questions. Mrs H replied '*how am I supposed to answer this…no.'* The advisor then asked whether she had been asked to move her funds to a safe account and Mrs H accepted that she had.

Mrs H did then try to go back on her answer and assure first direct that she had obtained a new car and had gardening work which she now needed to pay for. Mrs H was passed on to a second advisor, who asked Mrs H again if she'd been told to move her money to a safe account to protect her from fraud. Mrs H acknowledged at this point that the FCA had contacted her, and at this point the scam was uncovered. Only one payment was therefore made to the fraudsters for £20,000, and Mrs H's loan funds have since been returned without a loss being incurred by Mrs H.

First direct raised a fraud claim for Mrs H and subsequently considered its liability to refund Mrs H. First direct 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. First direct says one or more of those exceptions applies in this case.

First direct has said Mrs H didn't have a reasonable basis for believing she was making a legitimate payment. It said it had warned Mrs H the day before about scenarios similar to this, but that Mrs H has proceeded in spite of this. First direct also said Mrs H ignored an 'effective warning' when making the payment to the fraudster, despite selecting the incorrect payment purpose. First direct has said that if Mrs H had chosen the correct payment purpose when making the first transfer ('unexpected request from bank/police/organisation'), its warning would have stated ***'STOP, this is a scam',*** and provided information more accurate to Mrs H's circumstances.

Mrs H remained unhappy and referred her complaint to our service. An investigator considered the complaint and upheld it in part. He didn't think Mrs H had a reasonable basis for believing the payment she made was legitimate. However, he also didn't consider first direct had done enough to protect Mrs H from financial harm from fraud, considering the fraud risk her payment presented. He therefore considered both parties should share liability, with first direct refunding Mrs H 50% of the payment she made.

First direct disagreed with the investigator's view. It considered that it had warned Mrs H about the scenario she fell victim to less than 24 hours before it then occurred. It thought that by choosing the incorrect payment purpose, its ability to protect Mrs H had been diminished. First direct didn't agree that a call was required to Mrs H at the time she made the first payment. First direct accepted this was a one off larger payment, but noted the payment reference provided was 'car', which is a genuine reason why someone may make a larger payment. It considered that even if it had called when Mrs H made the first payment, there wouldn't have been the same level of suspicion at this point regarding the payment, as only one payment had been made and no loan applications. It considered that Mrs H would have been able to provide plausible answers to questions it posed regarding the 'car' payment transfer.

Mrs H also thought she should receive a full refund of her losses. She considered first direct should have stopped the first payment she made. She also made reference to the Payment Systems Regulator reimbursement scheme that comes in from October 2024, which she considers it fair to be applied to her complaint also.

As both parties disagreed with the investigator's view, the complaint has been referred to me for 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.

First direct 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 authorised push payment (APP) scams in all but a limited number of circumstances.

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.*

First direct considers Mrs H didn't have a reasonable basis for believing she was making legitimate payment transfers as part of the scam. Having considered the information provided by both Mrs H and first direct, I think it is fair for first direct to have relied on this exception of the Code. I don't doubt that the scam Mrs H fell victim to was sophisticated in nature, taking advantage of the information Mrs H had provided the day before in order for it to appear more realistic and also preying on the fear and pressure caused from Mrs H considering her funds were at risk. I can also appreciate why the text she received would've provided reassurances that the caller was genuine.

However, I've also considered that Mrs H has herself acknowledged that she had a 'gut feeling' that something wasn't right, and felt uncomfortable several times on the call but proceeded in spite of this. She also raised a number of elements of the scam that seemed questionable – for example the fraudster's impatience when an earlier payment attempt timed out - and being coached on how to answer questions from the bank. I therefore think Mrs H did have doubts about the legitimacy of the caller throughout the scam, but proceeded in spite of these concerns and for this reason, Mrs H should be held responsible, at least in part for her losses.

I've then gone on to consider whether first direct should also be held responsible in part for Mrs H's losses. First direct has said the warning it provided Mrs H warned her that if she had been told which payment option to choose this was a scam, and had Mrs H taken heed of this, it would have stopped the scam from proceeding. First direct also said it's ability to protect Mrs H from the scam was impeded by her selecting the incorrect payment option. While I agree this is true, I've also taken into account that the provision of an effective warning is the minimum expectation required of a firm when faced with an identified fraud risk. In this case, Mrs H's first payment to the fraudster was for £20,000. This was significantly higher than any other payment she had made in the 12 months prior to the scam. I therefore think that the risk of financial harm from fraud was such that first direct ought to have intervened to a greater extent than a written warning and requested to speak to Mrs H, prior to allowing the payment to proceed. First direct has argued that Mrs H gave a genuine reason why someone may make a one off larger payment as the payment reference (a car). I don't think this removes any onus on first direct to ensure itself that firstly, that was the genuine payment purpose (as banks are well aware that customers are often provided with cover stories as part of a scam), and secondly, that even if it was the genuine purpose, that Mrs H still wasn't at risk of a scam related to this payment.

First direct has argued that even if it had spoken to Mrs H, any perceived risk would have been less than during the subsequent call, as there were less identifiable red flags at this point. While I accept this to also be true, I would nevertheless expect that for a payment as sufficiently out of character as this, first direct would've probed Mrs H both on the perceived payment purpose (the purchase of a car), as well as more general questions – as it did in its later call.

When Mrs H was questioned in the subsequent call, she confirmed when first asked by first direct that she had been told to move funds to a safe account. She also appeared uncomfortable when questioned on whether she had been coached in answering first direct's questions and I think her response to this question was also a red flag. First direct has suggested that our service is relying purely on speculation regarding what Mrs H would or wouldn't have said if questioned on the first payment. However, as first direct *didn't* contact Mrs H when I consider it reasonably should have, I can only rely on what I think is likely to have happened, should first direct have intervened when I consider it should have. The subsequent call it had with Mrs H is the most reliable evidence available to determine how Mrs H would have reacted, had first direct called less than an hour earlier. While Mrs H clearly had a cover story provided by the fraudster, she also told first direct the truth almost immediately when questioned. I therefore think it's more likely than not that had first direct probed Mrs H on this first call, it would’ve come to light at this point that she was falling victim to a scam.

Lastly I’ve considered Mrs H’s point that the Payment Systems Regulator reimbursement scheme should be applied to her case, considering its upcoming application. However, the scheme referred to is not intended to be applied retrospectively and so it would not be fair to apply such considerations to bank’s actions, prior to the scheme’s start date.

Overall, for the reasons I’ve explained, I think both parties could reasonably have done more to prevent the scam from occurring, and I therefore think it’s fair for liability for Mrs H’s losses to be shared equally between both parties.

My final decision

My final decision is that I uphold Mrs H’s complaint against HSBC UK Bank Plc trading as first direct in part, and I require it to:

- Reimburse Mrs H 50% of the £20,000 she lost to the scam (totalling £10,000)

- Apply 8% simple interest, from the date Mrs H made the payment until the date of settlement.

Under the rules of the Financial Ombudsman Service, I’m required to ask Mrs H to accept or reject my decision before 1 July 2024.

Kirsty Upton
Ombudsman