DRN-4058518

The complaint

Ms C complains that HSBC UK Bank Plc (trading as 'First Direct') has refused to refund her in full for transactions totalling approximately £5,500 which she said she did not make or otherwise authorise.

What happened

I issued a provisional decision in March 2023 to explain why I thought Ms C's complaint should not be upheld. And I said I would consider anything else that either party wanted to give me prior to reaching a final decision in this case. This is an extract from my provisional decision:

"The details of this complaint are well known to both parties, so I won't go into every detail of what happened here. But in summary, Ms C says First Direct have declined to refund her in full for three payments totalling approximately £5,500 that she says she did not make or otherwise authorise. First Direct think it is most likely that she did make the payments, but as a part of a scam, and offered to refund 50% of the £3,900 payment.

Ms C said that in December 2020 she received a text message claiming that she was owed a tax rebate and providing a link to click on for further information. Ms C said she clicked on the link but realised it could be a scam, so she did not enter any personal information. Ms C said she later received a call from someone purporting to be from First Direct. She explained they asked a security question she knew First Direct did not ask – for part of her date of birth. She terminated the call without divulging any of her personal information to them. She decided to call First Direct about half an hour after this call to let them know what had happened as she said she was concerned about the risk of fraud. She said whilst she was on the phone to them she looked on her phone and saw that funds had left her account. £3,900 of the money went to an unknown third party's account, and the remaining funds went to her own account held with another business and were then sent on from there to an unknown third party's account.

Ms C denies making or otherwise authorising any of the payments from her First Direct account, or the account held with the other business. Ms C thinks that First Direct should have prevented the payments from taking place – she said they blocked a legitimate payment of around £1,500 a few months prior to this three times. So, she complained to First Direct, who didn't agree that these were unauthorised payments. First Direct think it is most likely that Ms C fell victim to a scam and sent the payments herself thinking she was protecting her money by sending it to a 'safe account'. First Direct said the payments required access to her online banking, which was done on her device and using her facial recognition ID, but Ms C says she does not know how her device or personal banking information could have been compromised. She explained that no one else has access to her phone or any of her security details, so she thinks she may have been hacked.

So, they considered her case as an authorised push payment scam, under the Contingent Reimbursement Model Code. They refunded 50% of the payment to the unknown third party account but didn't refund the payments made to her own account with another business as the loss happened on the other account when they were sent on.

Ms C was unhappy with First Direct's response, so she brought her complaint to our service. One of our investigators looked into what had happened and recommended that First

Direct's offer was fair and reasonable in the circumstances. They agreed that on balance it was more likely Ms C did authorise the payments – and most likely as the result of a scam. They said that the payment of £3,900 to a new payee could be considered under the CRM code, but not the others as they went to an account in her own name and so the loss took place there. They said that they could not conclude that Ms C had a reasonable basis for believing that the payments were legitimate, but that as First Direct had accepted that they had not provided an effective warning the offer to refund the 50% of the £3,900 payment was fair and reasonable in the circumstances. Ms C did not agree and responded through her representative. In summary, they said:

- *Ms C had not made the payments, and had to flag them as fraudulent to First Direct.*
- *She had not been able to provide any evidence of the phone being hacked because they were not experts in this field and therefore have no idea how a third party could have done this.*
- *Ms C had never given First Direct her facial image so they were unclear as to how they could verify it was her.*

Our investigator's opinion on the matter did not change, so the case has been passed to me to decide.

What I've provisionally 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 the 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.

And where there is a dispute about what happened, and the evidence is incomplete or contradictory, I will reach my decision on the balance of probabilities – in other words, on what I consider is most likely to have happened in light of the available evidence. My appraisal of the available evidence has led me to reach broadly the same conclusions as our investigator – and for largely the same reasons. However, I will be referring to evidence that was not put to Ms C in the investigator's opinion, so both parties will have a further opportunity to provide submissions and evidence prior to me reaching my final decision. But, I will explain the decision that I am thinking of reaching based on the current available evidence.

Due to the disagreement between First Direct and Ms C about what happened, I have reviewed the evidence carefully, including the evidence from the other bank that some of the money went through before going onto a third party. Having done so, I think it is most likely that Ms C authorised the payments herself. In summary, this is because:

- *The bank provided the technical evidence which shows that Ms C's device – or certainly the same device that has been used for undisputed transactions – was used to make the payments. Ms C's testimony is that she had this device with her, and no one else had access to it.*
- *Ms C's own testimony is that she received a text message and opened a link – though provided no personal information at this time. She said she then received a phone call from someone purporting to be from First Direct – which seems most likely to have been from the scammer. She said she did not divulge any personal information on this call either. It seems unlikely that the scammer would have called her if they already had the means to make these transactions on her behalf – such as through malware or similar. So, it would be reasonable to conclude that opening the link in the text message was not enough to give someone access to her phone or*

account. Therefore, if she had not divulged information to the person who called her, it does not seem there was a point of compromise for her banking details or her phone.

- *According to the complaint notes from First Direct, the scam was first reported on 9 December 2020. The note says she "was contacted by fraudsters masking first direct number they mentioned that a number of fraudulent transactions had been attempted on her account and that she will need to move the money to a temporary safe [account.] [Ms C] did a number of internal transfers so all her money was in her first [direct] account and then made [a transfer to a third party account] and two [transfers] to her own [third party business] bank account she was further advised to move back her money from the [third party business] account to a account that had been set up for her. [Ms C] rang bank to check if the payment sent from [third party business account] had been received by [First Direct].*
- *Further to this, the evidence from the third party business who Ms C holds an account with says that she completed a fraud report which said that she had been called earlier telling her to transfer money from her account to her other account and then onto the third party payee, but that she now knew this was fraud. Her testimony to the third party bank changed the next day when she said it was not her.*
- *I appreciate that Ms C denies saying this, and indeed told both businesses the following working day that she did not make the transactions – but it seems unlikely that two unrelated banks would have recorded the same erroneous information about the scam and how it unfolded. And I see no reason for a third party fraudster with access to both her bank accounts to report the scam.*
- *The series of events as evidenced and described in part by Ms C also fit the hallmarks of a common type of scam – a safe account scam. I say this because they often do unfold by someone being tricked into following a link in a text message, before speaking to someone purporting to be from their bank who persuades them that their money is at risk and they need to move money to a safe account. Here, Ms C does tell us that she received this kind of text, and this kind of call, and her initial fraud reports suggest she was persuaded to send the money on to a 'safe account'.*

So, when considering all of this I do think on the available evidence I am likely to say that it is most likely that Ms C authorised these transactions herself.

Should First Direct refund any of the losses?

In broad terms, the starting position in law is that a bank is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of their customer's account. However, where the customer made the payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse them, even though they authorised the payment.

In this case, First Direct were suitably persuaded that Ms C fell victim to an authorised push payment scam that they took the decision to consider the case under the Contingent Reimbursement Model code (the 'CRM code'). As they have done so, and as I am minded to say I think the payments were made as the result of an authorised push payment scam too, I will also consider whether their offer was fair and reasonable in the circumstance of this complaint.

The CRM Code

First Direct are a signatory to the Lending Standards Board Contingent Reimbursement Model ('CRM') Code which requires firms to reimburse customers who have been the victims of APP scams in all but a limited number of circumstances. The code does not cover payments made to an account in the customer's name and control as the loss did not

happen on the first account – so I have only considered the £3,900 to a third party here. Ms C would not be entitled to a full refund under the code if First Direct can fairly and reasonably demonstrate that Ms C has failed to meet the requisite level of care under one of more of the listed exceptions set out in the CRM Code.

Those exceptions are:

- *The customer ignored an effective warning in relation to the payment being made;*
- *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.*

**There are further exceptions within the CRM Code, but they do not apply in this case.*

In this case, First Direct has accepted it did not provide effective warnings about the payment. This is why they have offered to refund 50% of this payment. As this is not in dispute, I see no need to go over this here.

Did Ms C have a reasonable basis for believing she was sending the funds to a legitimate business?

It is for First Direct to establish that a customer failed to meet a requisite level of care under one or more of the listed exceptions set out in the CRM Code. The exception relevant to this case is where 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.

Given what I think most likely happened in this case on balance, I do not think that it is likely that Ms C did sufficient checks to ensure she was sending money to First Direct. On the available evidence I am likely to decide that she fell victim to a 'safe account' scam – where someone called her purporting to be from First Direct and told her that her account was at risk and so she had to move her funds on. If this is what happened, I would have expected her to think it strange that she was asked to send money directly to a 'safe account' in someone else's name. As she denies that this is what happened, I have no evidence to suggest she was provided with a compelling reason for this. If this is what happened, she was also asked to send some of the funds to her own bank account with the third party business, from where she sent it on to the scammer. I would expect this to give someone cause for concern if they thought they were dealing with their own bank, who had set up a safe account. Again, I have no evidence that the scammer provided a compelling reason for why this had to be done. So, on the evidence that I have I am likely to say that I think it was fair and reasonable for First Direct to conclude that Ms C did not have a reasonable basis for belief here – and so it would be fair to deduct 50% of the payment.

Should First Direct have done more to protect Ms C?

In addition to their responsibilities under the CRM code, when Ms C made the payments First Direct should fairly and reasonably have had systems in place to look out for unusual and out of character transactions or other signs that might indicate that Ms C was at risk of fraud or financial harm (amongst other things).

I've considered whether any of the payments should have flagged as unusual or out of character – and I am not minded to say that they ought to have. Whilst the first payment was not for an inconsequential amount, I do not consider a payment of £3,900 unusual enough that it ought reasonably to have put First Direct on alert that Ms C was at risk of fraud or financial harm such that further action would be warranted. However, there was a transfer into her account just before hand of £4,500 from another First Direct account, and 'safe account' scams often see customers move money from their savings into their current account (or similar) and then on to a scam account. So I have considered whether this

movement, and the subsequent payments should have given First Direct cause for concern.

I am not clear whether the transfer in cleared any other accounts she had internally – it appears they did not totally as there were a further two internal transfers. But there was still a significant sum remaining in Ms C's account after the £3,900 payment was made to the scammer – over £1,000. So, I don't think that at this point, First Direct ought to have recognised the risk of the scam. The subsequent payments of £1450 and £105.59 went to another account in her own name, held with another business. I think this means that First Direct may not have recognised them as linked to the first scam payment – and so I don't think they ought to have flagged as unusual or out of character and so I do not think they could have done more to stop the scam here.

Recovery of funds

I have also considered whether First Direct could have done more to recover the money once they had been alerted to the fraud or scam. We would expect a business to take reasonable steps to try and recover the money from the bank it was sent to. First Direct did try to recover the funds sent from Ms C's account to the third-party account – and were able to evidence they contacted the receiving bank. They were unable to recover any funds from this bank – who confirmed under a week later that no funds had remained in the account at the point First Direct contacted them. What remains unclear is the exact timing of the message from First Direct to the receiving bank – and so I request that this detail is provided by First Direct. If there was any delay in reporting this to the receiving bank and funds remained at the time they should have reported it, it is likely I will have to consider whether any further refund is due.

My provisional decision

On the available evidence, my provisional decision is that I think First Direct's offer was fair,

and as this has been paid already I would not be asking them to do anything further."

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.

Ms C's representative responded on her behalf. In summary, they said:

- They wanted this case to be considered along side the case that has concluded against the other business Ms C had a personal account with (the one where one of the payments was sent). The other business had not refunded any of the loss – and they spoke more about specifics of that complaint.
- Ms C maintains she never clicked on any link, never moved any money. Her only attempt was to contact the two banks to advise this was happening. No one would have access to Ms C's phone other than herself.

I have thought about these points, and they have not changed my thinking as outlined in my provisional decision. On the first point about the other business – this complaint has been decided by way of a final decision issued by another ombudsman so this case is now closed. I appreciate Ms C feels there is some disparity between the two cases, but as I outlined in my provisional decision I have considered First Direct's offer to reimburse 50% of the payment to an external account based on the rules outlined in the CRM code, and assessed that it was fair in the circumstances. My role is to decide this case on the specifics of what happened here – and I have taken into account the evidence on the other complaint but I am bound to decide this case on its own merits.

With regard to the fact Ms C maintains she didn't click on any link or move any money – I have dealt with this extensively in my consideration of this case and in the provisional

decision. I am afraid my conclusion remains the same, for the reasons I outlined in my provisional decision.

First Direct did not provide any comments on the provisional decision itself. I asked First Direct to evidence whether they had reported the scam to the receiving bank in a suitably timely manner. They have provided evidence that the notification went to the receiving bank around the day after I would have expected them to. But, having spoken to the receiving bank, the funds from Ms C's transfer, as well as other victims, had been quickly moved on and the account had been blocked before First Direct even got in touch. So I do think they could have moved with more haste to recover the funds, but I cannot say that it would have made a difference here.

My final decision

I think that HSBC UK Bank Plc trading as first direct made a fair offer, and as they have already paid this to Ms C I require them to do nothing further.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms C to accept or reject my decision before 27 April 2023.

Katherine Jones
Ombudsman