DRN-3212241

The complaint

Mrs M is unhappy HSBC Bank Plc (trading as "First Direct") hasn't reimbursed her after she was the victim of a scam.

What happened

In January 2021 Mrs M's partner was contacted claiming to be from the fraud department of Bank A. They said his money was at risk and he wouldn't be protected unless he moved his money immediately. Mrs M also had an account with Bank A. Mrs M has said they were sceptical about the legitimacy of the call and asked the scammer to verify where they were calling from. The scammer gave them a mobile number they could call back on with a name and a password.

Mrs M spoke to the scammers the following day and they convinced Mrs M and her partner that they were calling from Bank A's fraud team. They said corrupt staff at Bank A were accessing their accounts. They persuaded Mrs M during these calls, which took place over three days, that her First Direct account was also at risk.

Mrs M was told she could help by transferring money from her account into the corrupt staff members accounts, so the fraud team could monitor the activity. She was told she would get this money back within a week and policeman would be visiting her home to assist.

On 28 January 2021, around three days after the scammer initially contacted her and her partner, Mrs M sent payments of £3,000 and £4,000 from her First Direct account to two different accounts that belonged to the scammers. Mrs M instructed the payments online and says that when warnings appeared the scammers told her to ignore them as they didn't apply to her.

The payments didn't arrive in the scammers account immediately so under the scammer's instruction Mrs M called First Direct to ask what was happening. She was told the payment would take two hours to appear. Two hours later she contacted it again when the payment hadn't appeared in the scammers account to ask when the money would be moved. She'd been coached by the scammers to provide cover stories around the payments so First Direct, believing what she'd told it, allowed the payments to go through.

Mrs M later realised she'd been the victim of a scam. She reported the matter to First Direct but it didn't think it was at fault. Mrs M was unhappy with its response and brought the complaint to our service to consider.

Our investigator concluded First Direct should reimburse Mrs M for 50% of her loss as it shared some liability under the relevant regulations. They didn't feel First Direct had provided sufficient warnings to Mrs M when she made the payments as it was required to. First Direct didn't agree so the complaint has been passed to me to make 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.

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.

First Direct has signed up to, and agreed to adhere to, the provisions 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. 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.

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.

Did Mrs M ignore effective warnings?

The CRM code says that, where firms identify APP scam risks, they should provide effective warnings to their customers. The code sets out that an effective warning should enable a customer to understand what actions they need to take to address a risk and the consequences of not doing so. As a minimum, the CRM code sets out that an effective warning should be understandable, clear, impactful, timely and specific. First Direct feels it gave Mrs M effective warnings in this case. It says these were given both when she instructed the payment online and then again when she called it to try and rush the payment through.

I've listened to a recording of the call in which First Direct says it gave Mrs M an effective warning and I don't think the conversation it had with her was clear or impactful enough to be an effective warning in these circumstances.

First Direct asked if Mrs M had been contacted out of the blue by someone asking her to make the payment and asked her to move money to a safe account. But it didn't explain more about safe account scams and how they tend to be perpetrated or that scammers pretend to be from customers' own banks or that they claim to be trying to catch corrupt staff members. It also didn't explain any steps Mrs M could take to avoid falling victim to this kind of scam, such as calling her bank back on a legitimate number to check what she was being told.

Whilst I accept Mrs M wasn't honest with First Direct about what the payment was for – she said she was making a payment to her nephew – I don't think it's uncommon for victims to be coached into giving cover stories. I think it ought to have seemed unusual to First Direct that she was phoning to try and rush the payment through. And whilst she said the payment was for her nephew I don't think she provided a plausible explanation as to why the payment needed to be immediate or why she was so worried about the two hour delay. This kind of pressure is something I'd expect First Direct to be on the look out for as an indication someone might be the victim of a scam.

First Direct has also said Mrs M ignored the effective warnings it gave when she instructed the payments online. Mrs M has told this service that she remembers seeing the warnings but the scammer was walking her through the payment instruction. And when the warnings started to appear they instructed her to ignore them.

I've considered the warnings First Direct provided, and its subsequent submissions around why it feels they were effective in line with the requirements of the CRM code. But I don't consider the warnings were effective, so I don't agree First Direct has met its obligations under the code.

The warning does say Mrs M should put the phone down if anyone asks her to move money and *"If someone calls you and asks you to move money – don't, even if it's another account you already have. Remember, we'll never ask you to send money to a 'safe account' or to another bank".* But again, I don't think this brings to life what a scam of this nature looks like or the sophisticated nature of the scam – so it lacks impact.

And it provides little detail about how safe account scams might work or how fraudsters impersonate bank staff and the kind of cover stories they provide. I don't think it effectively warned Mrs M to the extent she could apply any knowledge to her own situation which was slightly different to the one alluded to in the warning.

Overall I haven't found that Mrs M ignored effective warnings when making the payments to the scammers.

Did Mrs M have a reasonable basis for believing what she was told by scammers?

Having considered what Mrs M has said about what she was told by scammers very carefully, overall, I don't think she had a reasonable basis for believing what she was told. In reaching this conclusion I've taken the following into account:

- Scammers initially called Mrs M's partner, not Mrs M. And they don't appear to have had any personal information about Mrs M or her accounts that she might reasonably have expected her bank to have. They appear only to have involved her, and told her that her account was at risk because she started speaking to them on her partner's behalf.
- Mrs M says she was immediately suspicious and that she'd heard of 'safe account' scams. She told the scammer about her suspicions and in order to convince her, the scammer gave her a number to call back on. It doesn't appear the scammer claimed this number could be looked up online or otherwise verified as an official Bank A number and was actually a mobile number. So it's not clear why Mrs A felt this was persuasive or offered any assurance this meant they were calling from Bank A.
- I don't think Mrs M has been able to explain why she was convinced she thought corrupt staff at Bank A would be able to access her account with First Direct. Whilst I understand why she thought they might know about the account if she'd transferred money between them, I don't think this explains how she thought they would be able to access this account when they work for a different bank.

- Whilst I don't think the warnings given to Mrs M were effective as defined by the CRM code, I do think some of the things she was told, both online and when she spoke to First Direct on the phone, ought to have given her cause to think about things more carefully. And I would note that she'd also spoken to Bank A during this period, which had also given her information about this type of scam that was relevant to her situation.
- I understand Mrs M has said she felt under a lot of pressure and she was worried about losing her money. But it's also clear the scam, which involved her partner and several accounts, took place over three days. So although I do accept scammers are skilled in applying pressure, I think it's clear there was time in between interactions with the scammers where Mrs M could try and verify some of what she was told.
- It's also not clear why, given the alleged urgency of the situation, Mrs M accepted that her money would be safe while the scam was ongoing. For example it seems the scammers told them the money would be safe overnight after the initial call when arranging to call back the next day but it's not clear why they would know this if the accounts were under attack from fraudsters.

Overall, I don't think Mrs M had a reasonable basis for believing the payments she was making were genuine so she is partially liable for her loss.

Could First Direct have done more to recover Mrs M's money?

First Direct has said that Mrs M contacted it on 28 January 2021 at 6.26pm to report she thought she'd been the victim of fraud. I think First Direct needed to act immediately, not the next day as First Direct has suggested, in contacting the beneficiaries' accounts to try and recover the funds she'd lost. First Direct confirmed it didn't do this so it hasn't acted as I would've expected in this case.

But, when considering whether appropriate action on First Direct's part would've resulted in the successful recovery of the funds, I have to consider the receiving bank's actions too. This is because First Direct would've been relying on the receiving banks to respond to its requests. First Direct didn't contact the beneficiary banks until 11 February 2021 – long after the scam was reported to it and it should've taken action. We've independently contacted the receiving banks to find out when the money was removed from the accounts and whether, had First Direct acted immediately, this likely would've resulted in the return of the funds.

In the case of one receiving bank, it responded the day First Direct contacted it and asked for further evidence relating to the scam, which First Direct provided the same day. So it's clear it needed to investigate things before it was able to return the funds. This bank has sent us evidence that the money was moved from the account the same day it was credited, and given it always would've needed to investigate things before responding to First Direct, overall I think it's unlikely the delay caused by First Direct prevented the return of any funds sent to this account.

The other receiving bank asked for more time to investigate the matter. It responded on 24 February 2021 to confirm the funds couldn't be retrieved. We've contacted this bank for more information about what might've happened had the scam been reported immediately as it should've been. And the information it's provided show the transactions that resulted in the funds leaving the account were all carried out before Mrs M reported the scam on 28 January 2021. So the money was effectively already gone before First Direct could've contacted it.

Overall, First Direct's delay in contacting the receiving banks hasn't caused a loss in this case.

Redress

As First Direct didn't provide Mrs M with effective warnings, under the CRM code, it needs to reimburse her for 50% of her loss.

As the money came from Mrs M's current account and she's deprived of the use of the funds, simple interest should be added to this amount from 5 March 2021 (when First Direct concluded its investigation) until the date of settlement at a rate of 8%.

My final decision

I uphold this complaint and direct HSBC Bank Plc to pay Mrs M the settlement outlined above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs M to accept or reject my decision before 12 August 2022.

Faye Brownhill
Ombudsman