DRN-4643631

The complaint

Company K ("K"), complain that Starling Bank Limited ("Starling") won't refund the money that was lost as the result of an Authorised Push Payment ("APP") scam.

Mrs T brings the complaint on behalf of K, for ease of reading I will mainly refer to Mrs T throughout this decision.

What happened

I issued my provisional decision on this complaint on 6 February 2024. The background and circumstances of the case and the reasons why I was minded to not uphold it were set out in that decision. I have reproduced the provisional decision in italics below:

In December 2022, Mrs T received a message from what appeared to be her other banks fraud team. The message asked Mrs T to call back, which she did but there was no answer. In the early hours of the morning Mrs T then received a call, again saying that it was from her other banks fraud team. Mrs T asked how she could be sure it was them and they directed her to check the number that was calling her with the number on the back of her bank card, with the numbers matching.

Mrs T explained that because the number she was being called on matched her banks and as they knew some of her personal details, she believed the caller was legitimate. She added that she also received a message from what appeared to be another bank, that K held an account with, indicating that a loan had been applied for. This further convinced Mrs T that her accounts were at risk, as she hadn't applied for a loan. But unknown to Mrs T at the time, this was a fraudster impersonating her bank.

The fraudster persuaded Mrs T that her bank accounts were under attack by a Trojan virus and she needed to move her money to safe accounts, in order to protect it. The fraudster instructed Mrs T to download remote access software to her PC to enable them to guide her through this. Believing she was speaking to her bank, Mrs T followed the fraudsters instructions and, on 16 December 2022 made a payment for £4,378.90, from the business account K held with Starling, to account details that the fraudster provided. Mrs T also transferred a significant amount of money, from accounts K held with other banks, to accounts the fraudsters controlled.

Mrs T began to feel uneasy when the fraudster asked if she had any foreign accounts. Following which she carried out an online search and saw an article about a scam that matched what had happened to her.

Mrs T raised the matter with Starling, who looked into K's complaint, but didn't uphold it. In summary it felt it had provided sufficient warnings when the payment was made. It also didn't think Mrs T had a reasonable basis for belief. Once the scam had been reported, Starling reached out to the beneficiary bank (the bank to which the payment was made) to see if any money could be recovered. But it was only able to recover £3.10, which was returned to K's account.

Unhappy with Starling's response, Mrs T brought K's complaint to this service. One of our Investigator's looked into it but didn't think the complaint should be upheld. In summary it was our Investigator's view that Mrs T didn't have a reasonable basis for belief. As well as this, our Investigator thought that whether the warnings provided were effective or not wouldn't have made a difference, as Mrs K wouldn't have seen them.

Mrs K didn't agree with our Investigator's view. As agreement couldn't be reached the complaint has been passed to me for a decision.

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 a complaint, I'm required to take into account relevant: law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been 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 it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account.

But, 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 Starling should have reimbursed K in line with the provisions of the Lending Standards Board's Contingent Reimbursement Model (the CRM Code) it has signed up to and whether it ought to have done more to protect K from the possibility of financial harm from fraud.

There's no dispute here that Mrs T was tricked into making the payments. She thought she was speaking to her other bank's fraud department, and this wasn't the case. But this isn't enough, in itself, for K to receive a full refund of the money under the CRM Code.

The CRM Code

Under the CRM Code the starting principle is that a firm should reimburse a customer who is the victim of an APP scam, like Mrs T. The circumstances where a firm may choose not to reimburse are limited and it is for the firm to establish those exceptions apply. They are:

- *the customer ignored an 'effective warning' by failing to take appropriate steps in response to that warning; or*

- *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 that*
    - *the person or business with whom they transacted with was legitimate.*

There are further exceptions within the CRM Code, but they do not apply in this case. The CRM Code also outlines the standards a firm is expected to meet. And it says that when assessing whether the firm has met those standards, consideration must be given to whether compliance with those standards would have had a material effect on preventing the

APP scam that took place.

Did Starling meet its obligations under the CRM Code?

Firstly, in the circumstances of this case, I'm satisfied that the requirements of the effective warning exception have not been established.

The nature of this type of scam means that in general an on-screen warning would need to have enough impact to stop someone from continuing to follow urgent instructions they believe originate with their bank. Otherwise a warning is unlikely to have a reasonable prospect of "positively affect[ing] Customer decision-making in a manner whereby the likelihood of an APP scam succeeding is reduced" – as required by the CRM Code.

I'm mindful that, in part, the warning Starling provided was relevant to the scam that Mrs T fell victim to, in that it details that Starling will never ask a customer to move money to keep it safe and that fraudsters can make calls appear to come from different numbers.

And while I consider that in some circumstances the warning shown here could have an impact, I don't think it was sufficiently impactful to be generally effective against this type of safe-account scam.

Specifically, there's a lot of text within the warning, which during a safe account scam could be difficult to follow. The warning is also not particularly direct, personal or clear which is essential in a safe account scam – particularly so given the level of coaching that's often involved in this type of scam and the fact the consumer genuinely thinks they are speaking to the bank.

I also don't think the explanation of spoofing is clear enough. I don't think it really gets across the point, that scammers can make phone numbers look like the genuine bank's phone number or a very similar one – and in particular make it clear that it is a common safe account scam feature. It also puts the onus back on the consumer to identify whether it's a scam by saying 'if you're in doubt' when in fact, it should be more direct in confirming that such scenarios are highly likely to be or will be a scam.

Typically, this type of scam operates at pace and under pressure. The victim believes they are speaking to someone trusted, someone based in the fraud team of their bank. A scammer will typically suggest the need for urgency. The potential impact of an in-app warning is thus reduced, and there is a greater chance that the victim won't read the message fully, as was the case here. This is especially so given the pressure they are typically under.

With the above in mind, I don't consider the warning Starling gave here fully met the requirements for an Effective Warning under the CRM Code. It follows that Starling cannot fairly apply the Effective Warning exception to K's case – it hasn't demonstrated that such a warning was provided.

Did Mrs K make the payments without a reasonable basis for belief?

I've gone on to consider whether Starling has been able to establish that Mrs K made the payment without holding a reasonable basis for believing what she did at the time.

The CRM Code specifies that all the circumstances at the time (to include the sophistication of the scam) need to be taken into account. I also consider that any warning or other messages provided are relevant circumstances - even where those warnings weren't Effective Warnings (as I have found here).

Firstly, I consider that the scam here was relatively sophisticated and persuasive. It involved phone number 'spoofing' to mimic multiple bank's real phone numbers, along with multiple calls and messages and remote access. From what I've seen I don't think Mrs T has proceeded with a complete disregard to risk and she asked the caller how she could know it was them calling. She was persuaded, amongst other things, by the number she was called from matching the number on her bank card and by the caller knowing some of her personal information. Based on what I've seen, I'm persuaded that in all the circumstances here, Mrs T had a reasonable basis for believing she was speaking with one of her banks and following its instructions to transfer money to a safe account it had created in order to protect her.

What's more, Mrs T has described how the call from the fraudster was received in the early hours of the morning. Her occupation means Mrs T had been working long hours and she's explained how she had been deprived of sleep, so it's understandable why she may have been distracted and caught off guard. =

I agree with Starling that parts of the text of the warning messages it showed were relevant to the scam that occurred here. But in the circumstances here, Mrs T was already under the spell of the scammer and in any event she doesn't recall seeing the warning message at the time. I don't find that unreasonable given what she has said was happening at the time. She was being guided by the fraudster and indeed, with the use of remote software, it appears the fraudster has moved through some of the payment process without Mrs T's intervention. Unfortunately, it seems that here the urgent promptings of the caller (whom Mrs T believed was from her banks fraud team) were more impactful in the moment than Starling's fraud warning message.

I'm not persuaded that Mrs T should fairly be blamed for falling for the fraudster's story. I can understand why she accepted what she was being told. I consider it critical in this situation to apply appropriate weight to the trust built by the scammer during the course of this scam, and the sophistication of the mechanics of the scam. And in particular, I find that a spoofed number can often prove a very powerful deception to convince a customer.

All taken into account, in this specific instance I'm satisfied this carried significant weight – adding considerable legitimacy to the false beliefs the scammer was able to engender. At the time Mrs T believed she was speaking to her bank, and I don't think she ought to have realised that she wasn't.

I appreciate to the trained eye and with the benefit of hindsight, there may have been some 'red flags'. In particular that Mrs T was told by the fraudsters to leave the room while they had access to her PC, she was told this was to avoid the potential for those who were attacking her account being able to infiltrate the conversation. While in the cold light of day Mrs T may look back and have done things differently, it is important to bear in mind the pressure she would have been under in the moment of a call like this. On balance, I believe that it was difficult for Mrs T to think clearly in the moment.

So, all things considered, I am not persuaded Mrs T acted unreasonably in the circumstances. Rather, I think she did what a reasonable person would most likely have done in the same situation. As such, I don't think it is fair to conclude that Mrs T didn't have a reasonable basis for belief.

Putting things right

For the reasons explained above, I'm currently minded to say that Starling Bank Limited should;

- *Refund K the money lost, being £4,378.90 (less any money that has already been recovered and returned to K).*

- *Pay 8% interest on this amount, from the date it declined K's complaint to the date of settlement.*

In my provisional decision I asked both parties to send me any further evidence or arguments that they wanted me to consider by 20 February 2024.

K responded and accepted my provisional decision and had nothing further to add. Starling confirmed it had received my provisional decision but didn't agree with it. In summary, it maintained that Mrs T didn't have a reasonable basis for belief and that it had provided warnings.

It said that Mrs T had been called by a different bank but hadn't been given any explanation as to what the connection was. Alongside this it said she was asked to move money to a safe account in a third party's name with a different bank. It also didn't think it reasonable for somebody to believe that a scammer could overhear a conversation that a person is having and being asked to leave the room the device was in.

Alongside this, Starling said the warnings it provided were specific to the customer and their situation. Overall, it thought there were significant red flags throughout the process.

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.

Starling has said that Mrs T ignored warnings it provided. But for reasons already explained in my provisional decision I don't find the warnings provided fully met the requirements of the CRM code. I'm also mindful that it's significant here that Mrs T was being coached by the fraudster, who also had remote access software, to act quickly and with urgency to protect her money. Considering she believed her money was at risk and that she needed to act promptly, it's understandable why she moved passed these warnings fleetingly.

Starling has maintained that it doesn't think Mrs T had a reasonable basis for belief when making the payment. But I don't think it was unreasonable for Mrs T to believe her money was at risk and that she was talking to her banks.

I've already explained in detail in my provisional decision why I think this to be the case. But I would add that I don't think its implausible for Mrs T to have believed that banks would work together to combat fraud. Mrs T has also said the manner of the way the fraudster spoke to her was similar to previous, genuine, experiences she'd had with her bank. She has pointed out that the fraudster knew personal information about her and that the bank's genuine telephone number had been replicated, which she had checked by looking on the back of her bank card – asking how she could be sure it was her bank calling.

It's also of importance to consider the individual circumstances of this case, whereby Mrs T is being called in the middle of the night and put under pressure to make payments to keep her money protected. The fraudster also knew step by step the actions Mrs T needed to take, which gave the caller credibility as they were able to describe the upcoming payment screens in a knowledgeable way.

I accept that there were some factors here that ought to have caused Mrs T pause for thought – such as why she was being asked to move away from the room she was in and that she was making the payment to an account in a different name to her own. But it's really important to remember that this didn't happen in the cold light of day.

I don't think Starling has given enough consideration to the fact the fraudster had created an environment where Mrs T thought she had to act quickly to protect her accounts from an attack. With the benefit of hindsight and the removal of the pressured environment, it's easier to identify elements where Mrs T may have had an opportunity to ask further questions. But I'm mindful that the convincing nature of these scams can often have a negative effect on a person's thought process and make them take steps that they might not otherwise take.

I say that particularly in the circumstances of this case, where Mrs T has been called in the early hours of the morning. Due to this and the nature of her job, she was both physically and mentally tired when this pressure was being applied. From what Mrs T has said, I am not persuaded that her actions were as a result of carelessness or indifference to what was happening, but rather deference to an expert that she believed was trying to assist her. In following their instructions (which in hindsight were clearly designed to divert her attention away from warnings and concerns) she appears to have believed she was simply carrying out instructions in the most expedient way possible.

Overall and on balance, I don't think Mrs T's belief was unreasonable. I think in similar circumstances a reasonable person would have acted in the same way Mrs T did here.

Putting things right

For the reasons explained above, I uphold this complaint and instruct Starling Bank Limited to ;

- Refund K the money lost, being £4,378.90 (less any money that has already been recovered and returned to K).

- Pay 8% interest on this amount, from the date it declined K's complaint to the date of settlement.

My final decision

My final decision is that I uphold this complaint against Starling Bank Limited.

Under the rules of the Financial Ombudsman Service, I'm required to ask K to accept or reject my decision before 24 March 2024.

Stephen Wise
Ombudsman