DRN-3429521

Complaint

Miss V is unhappy that Starling Bank Limited didn't reimburse her after she fell victim to a scam.

Background

The background to this case is well known to the parties so I don't intend to set it out in full.

Miss V has an account with Starling. In July 2021, she received a call saying that her identity had been stolen. The caller claimed to be a police officer and spoofed the number of the police force in her local area. Miss V's mobile phone had a caller identification functionality and so the caller display read 'Police Scotland' rather than the phone number itself. She was told that her personal details had been used to set up several accounts and that these had been used to launder the proceeds of crime. She was told that the security of her own bank account was compromised. She needed to pay her money into a secure account that would be controlled by the police.

She attempted to transfer the money she held in an account with a different bank, but the payment didn't go through. The caller suggested that she transfer the money into her account with Starling first. He suggested that she say that payment was to a friend. He persuaded her that to select the genuine reason for the transfer would risk alerting the fraudsters. She was told that she'd later receive a visit from a police officer who would explain how she could access her money. When there was no visit, she called the police who explained that she'd fallen victim to a scam.

She notified Starling straight away. Starling considered her complaint under the Contingent Reimbursement Model (CRM) code. It declined to pay a refund. It said that she didn't have a reasonable basis for believing that these payments were part of a genuine exercise being conducted by the police. The steps she was asked to take were at odds with the typical way the police operate – for example, she was asked to transfer money into an account that was in the name of a private individual, even though she'd been told she needed to put her money in a police account. She was also asked to send confirmation that the payments had been made via a social messaging app.

It also argued that there were further red flags that should've made her stop and think before proceeding with the payments. For example, she received a message saying that the 'Confirmation of Payee' process didn't match – i.e. that the name she put down on her payment instruction didn't match the name on the account she was paying. It thinks she ought to have had concerns about that.

It also said that it displayed Effective Warnings (within the meaning of the CRM Code) when she was making the payment. The warning essentially came in two parts. First, she was presented with the following text:

> *'Are you being told how to send this payment? Anyone explaining what buttons to click, or asking you to read the text on this screen out loud is a fraudster. If you continue, you could lose all the money sent.'*

She then had to answer a handful of questions about the payment. A further warning was displayed which said the following:

> *'Fraudsters will tell you how to answer these questions to scam you. A genuine organisation will never do this. A bank or any other organisation will never tell you to move money to a new 'safe' bank account. Fraudsters can make phone calls appear to come from a different number. Are you speaking with who you think you are? If in doubt you can call us on [number].'*

Overall, Starling considered that it had provided Miss V with an Effective Warning. It also noted that, under the terms of the code, Miss V wasn't entitled to a refund if she didn't have a reasonable basis for believing that the payments were legitimate. It was satisfied that was the case here and so it concluded that it didn't need to pay any refund.

Miss V was unhappy with this response and so she referred her complaint to this service. It was looked at by an Investigator who upheld it in part. The Investigator agreed that Miss V didn't have a reasonable basis of belief for some of the same reasons as outlined above. However, he didn't agree that Starling had met its standards under the code by providing an Effective Warning.

He said that the warning didn't give a good enough description of the number spoofing process. Although it says that fraudsters can make phone numbers look like they've come from a different number, it doesn't explain that they can make calls look like they're from an official number. In this instance, Miss V had a facility activated on her phone which automatically identified the call as being from Police Scotland. He also thought that parts of the warning were too vague – for example, including the phrase *"Are you speaking with who you think you are?"* The Investigator felt this suggested that the warning was trying to cover a wide range of potential scam types and was less impactful as a result.

Starling disagreed with the Investigator's conclusions. It said:

- The warnings make it clear that only a scammer would coach a customer through the process of making a payment by, for example, instructing them to select a particular reason for the transfer.

- It's clear that Miss V wasn't certain that she was genuinely dealing with the police. The warning told her to call Starling if that was the case, but she didn't do so.

- The explanation given in the warning about the process of phone number spoofing was sufficient.

- It's unreasonable to expect its warning to deal with every potential scam type and it was enough for it to make it clear that scammers can impersonate legitimate organisations and that such organisations won't instruct people to move their money.

Because Starling disagreed with the Investigator's opinion, the complaint has been passed to me to consider and come to a final decision.

Findings

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 have been good industry practice at the time.

The CRM Code 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 Starling to establish that a customer failed to meet their requisite level of care under 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 an *"Effective Warning"* by failing to take appropriate action in response.

- 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

There are further exceptions, but none are applicable in this case.

The warning Miss V saw when making the payment clearly contains a lot of detail that pertained to the scam she'd been targeted by. However, I'm not persuaded it meets the definition of an Effective Warning as set out in the CRM code.

The code says that warning must be specific. In this instance, I think it has fallen short. It doesn't cover the fact that a fraudster may present themselves as a representative of a legitimate public body, such as the police. A customer might be able to infer that from the content of the warning if given sufficient time to reflect. However, scams of this kind are usually presented to customers as if urgent action is required to keep their money safe and that can be a barrier to them processing the contents of the warning. I also find that the phrase *"Are you speaking with who you think you are?"* is too vague to impactful.

Nonetheless, I agree that Miss V didn't have a reasonable basis for believing that the payment was genuine. There were several red flags that ought to have given her pause for thought. I think she ought to have been concerned by the fact that the scammer asked for the money to be paid into an account in the name of a private individual and that confirmation of the payments should be sent via a social messaging app, rather than a more formal communication channel.

She received a "no match" warning regarding the name of the account she was paying. From what she's told us, I think she was concerned about this and had her doubts about the person she was talking to. However, she was given an explanation for the warning – she was told the account name must have been set up using that police officer's nickname. I think that explanation is far-fetched.

There's no doubt that Miss V sincerely believed that she was co-operating with the police. But I'm not convinced that belief was a reasonable one. As a result, while I don't think Starling needs to compensate her in full, I think it's fair and reasonable for there to be a 50% liability split between them.

Final decision

For the reasons I've set out above, I uphold this complaint. Starling Bank Limited should have partially refunded Miss V under the terms of the CRM code.

Starling Bank Limited should now pay Miss V:

- 50% of the money she lost to the scam, less the sum it was able to recover from the receiving account.

- 8% simple interest per annum on that sum calculated to run between the date it declined her claim under the CRM and the date it pays her a settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss V to accept or reject my decision before 8 November 2022.

James Kimmitt
Ombudsman