DRN-4016457

Complaint

Ms J is unhappy that Starling Bank Limited won't reimburse her after she fell victim to a scam.

Background

In April 2022, Ms J received a phone call from someone who claimed to be an employee of Starling's fraud team. They told her that there were security concerns regarding her account and that she needed to take prompt action to protect her money. Unfortunately, this call had not come from an employee of Starling, but a fraudster.

The scammer did several things to persuade Ms J that she was genuinely speaking to an employee of Starling. They referred to a recent suspicious phishing text message she'd received from Royal Mail. They took Ms J through a phony security process, asking her the same sorts of questions that she'd expect a genuine employee of the bank to ask. They also sent her a text message during the call that said *"You are on a call with an agent to discuss recent transactions"* and presented it as if the message had been sent by Starling.

The scammer told her that she needed to move her money to a "safe account" and that one had already been created for her with a third-party bank. That third-party has no connection to Starling, but the fraudster told Ms J that the two banks worked in partnership when it came to fraud prevention measures.

Ms J authorised the payments through the Starling app. A warning was displayed initially which said the following:

> *"Are you being told to make this payment? Anyone telling you what buttons to click, or asking you to read the text on this screen out loud is a criminal. You must not make the payment if you are being told how to answer the question or explain the payment. Read each question carefully and answer truthfully, otherwise you could lose all the money sent."*

The app then posed a series of questions about the payments she was making. It asked what the purpose of the payment was, how Ms J knew the recipient, whether she'd paid them before and so on. A second warning was then displayed:

> *"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' 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 call us .."*

Ms J says that the scammer seemed to know which questions were being displayed at each point during the process which affirmed her belief that she was genuinely dealing with an employee of the bank. She says she was talked through how to answer each question and the scammers stressed the urgency of the situation. She was told that the longer her money remained in her account, the greater the chance that she would lose it.

Once Ms J realised that she'd fallen victim to a scam, she notified Starling. It looked into things but decided to not reimburse her. It considered her complaint by applying the terms of the Lending Standards Board's Contingent Reimbursement Model ("CRM") Code. It said that she hadn't carried out sufficient checks before making the payment and it said that it had presented Ms J with effective warnings during the payment process. These clearly addressed the type of scam that she'd been targeted by and so she shouldn't have proceeded with the payments.

Ms J was unhappy with that and so she referred her complaint to this service. It was looked at by an Investigator who upheld it. The Investigator didn't think that the warnings displayed during the payment process met the code's definition of an *"effective warning."* She didn't think they were sufficiently specific and, although the second of the two warnings specifically uses the term 'safe account', she didn't think the warning did enough to bring to life what such a scam might appear like from the customer's perspective. She was also persuaded that Ms J had a reasonable basis for believing that the payments she was making were legitimate. The scammers had been able to do enough to convince her that they were genuinely calling from the bank's fraud department. In the Investigator's view, Ms J hadn't been careless to have been taken in by this.

Starling disagreed with the Investigator's view. It pointed out that Ms J had seen a warning which unambiguously asked if she was being told to make the payment. She'd also seen a warning which told her that, if anyone directed her as to how to answer the questions in the app, she should think twice before proceeding with the payment. As Starling disagreed with the Investigator's view, 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 doing so, 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 customer made a payment because 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.

The Lending Standards Board's Contingent Reimbursement Model code ("the CRM code") is of particular significance here. Starling isn't a signatory to that code, but it has agreed to adhere to it. It requires its signatories to reimburse customers who are victims of scams like this one in all but a limited number of circumstances. Starling says that one or more of those exceptions are applicable in this case.

Starling says that the following exceptions to reimbursement are applicable here:

- The customer ignored what the CRM Code refers to as an *"Effective Warning"* by failing to take appropriate action in response to such a 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.

I've considered the facts of this case carefully and I'm not persuaded that either exception is applicable here.

Warnings

First, I don't think that the warnings met the definition of *"effective warning"* under the code. It says an effective warning must be understandable, clear, impactful, timely and specific. The text of the warnings clearly had content that was relevant to this type of scam. If Ms J were given the time to have taken on board the content of the warning and process it, I'd have expected it to have an impact on her decision making.

However, for the warning to be impactful, Ms J needed time and mental space to process what the warning said. I've looked at how the warning was presented on the screen. I can see that Ms J would've been presented with the option to continue with the payment or to cancel. Those two options were next to one another. The layout of the warning page risked making it feel like an administrative part of the payments process that many customers simply click through robotically without thinking about.

That's a problem when attempting to prevent a scam like this. The approach of the fraudsters was to stop Ms J from pausing to think about what she was doing. I can see from the technical evidence supplied by Starling that the time between the first warning appearing on screen and the first question related to the payment being posed was a little over one minute. That doesn't necessarily mean that all of that time was spent reading the warning or thinking about its content. I'd expect there to be at least a very short lag-time between her proceeding past the warning and on to the first question. In addition to that, her testimony is that the fraudsters talked to her continuously throughout the process and stressed that time was of the essence. The longer she left the situation unaddressed, the greater the risk to her money. They'd successfully created a panicked state of mind in Ms J making it considerably more difficult for the warning to be impactful.

This is a known tactic for scammers when trying to reduce the impact of warnings on a customer's decision-making process. Having identified that there was a meaningful risk of Ms J falling victim to a safe account scam, the warning needed to take into account the likelihood that the scammers would attempt to reduce its impact in this way.

Reasonable basis of belief

I'm also satisfied that Ms J made these payments with a reasonable basis to believe that they were in response to a legitimate request from Starling.

The scammers knew enough to instil a false confidence in Ms J that she was genuinely speaking to her bank. They knew that she'd received a phishing text that looked like it was from Royal Mail. They were able to confirm the number on her card, that there'd been an attempted payment on that card and that it had been cancelled. The scammers were able to send her a text message that appeared to have come from Starling that looked like it confirmed that she was genuinely speaking to one of their employees. She also told us that the scammers seemed to know Starling's payment system very well and she assumed that only a genuine employee of the bank would have that degree of knowledge.

All the actions Ms J subsequently took must be seen in that context – i.e. that she sincerely believed she was following the instructions of her bank's fraud team. Starling has pointed to certain aspects of what she was being asked to do that she should've regarded with greater

suspicion. For example, the fact that she was being asked to make payments to accounts held with another bank or that those accounts appeared to be personal accounts in the name of specific individuals.

These things were explained by the scammers. The explanations that they gave carried more weight because Ms J had already been persuaded that this genuinely was a call from Starling's fraud team. I've already explained that I don't think Ms J was careless in believing that she was genuinely speaking to her bank, so I don't think I can reasonably say that she was careless for acting on the advice she believed the bank was giving her.

I'm also not persuaded that the warnings given during the payment process served to undermine the reasonableness of Ms J's belief that this was a legitimate request from Starling. As I explained above, I've found that the way the scammers coached Ms J through the process meant that she didn't take on board the contents of the warning. The fact that she didn't do so means that it can't have affected the reasonableness of her belief here.

Final decision

For the reasons I've explained above, I uphold this complaint.

If Ms J accepts my decision, Starling Bank Limited should reimburse the money she lost to the scam, less anything it has already refunded. It should also add 8% simple interest to that sum calculated to run from the date it declined her claim under the CRM until the date any settlement is paid.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms J to accept or reject my decision before 11 April 2023.

James Kimmitt
Ombudsman