DRN-4439329

The complaint

Mr B complains that Lloyds Bank Plc won't reimburse him the money he transferred to a fraudster.

Background

Mr B has explained that he received an instant message from who he believed was his daughter. The message he received stated '*Hi dad just broke my phone, getting a replacement tomorrow. This is my new number, can you save it right away?'*. Mr B didn't save the number at that time – he said he thought he could save it at a later date as and when his daughter called him. Around ten days later he received a text message from another number stating '*Hi Dad, save my new number.'* Mr B replied confirming he would. Unbeknownst to Mr B at the time, both messages were actually from fraudsters.

The fraudster went on to explain that she'd dropped her phone down the toilet, that it wouldn't turn on and she was scared she might lose her pictures and contacts, which Mr B provided some reassurance to her on. The fraudster went on to say her online banking has been frozen for 48 hours because of the number change and that she has an invoice of £1,850.50 which needs to be paid today to avoid additional charges. Mr B asked whether his daughter's husband could clear the invoice, to which the fraudster replied he couldn't. The fraudster asked whether Mr B could pay the invoice and she could pay him back within the next couple of days.

Mr B agreed to pay the invoice and the fraudster asked for details of who Mr B banks with before providing the account details. At this point Mr B has explained he was a bit doubtful, so tried to call the fraudster's phone number, but the call was unsuccessful – the fraudster stating the phone was *'messed up'* and for Mr B to text her instead. Mr B replied to this confirming he'd sent the money requested, but explained he *'wanted to make sure'* it was his daughter and that he'll call the landline. The fraudster advised she wasn't at home but provided details of Mr B's hair colour as reassurance it was really his daughter. However, Mr B has explained he was still suspicious, so rang his daughter's landline to see if she or her family were at home. When his daughter answered the landline, it became apparent Mr B had fallen victim to a scam. Mr B therefore contacted Lloyds to make a claim.

Mr B has explained his frustration that he had to call Lloyds around seven times to raise the claim, as he was being put on hold then cut off the call repeatedly. Mr B feels this impacted Lloyds' ability to recover his funds.

Once the claim was logged, Lloyds investigated Mr B's fraud claim and considered its obligations to provide Mr B with a refund. Lloyds is a signatory of the Lending Standards Board Contingent Reimbursement Model (CRM) Code which requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances. Lloyds says one or more of those exceptions applies in this case.

Lloyds has said Mr B didn't have a reasonable basis for believing he was making a genuine payment. Lloyds considers Mr B ought to have done more checks to make sure the person he was making the payment to was genuine. Lloyds has also said it provided an effective warning about this type of scam when Mr B made the payment, which Mr B ignored. The warning stated:

'Fraudsters are using WhatsApp to pretend to be someone you know and love.

Did a loved one text you, asking for money?

Did the text come from a new number?

If so, don't make this payment now.

First, speak to your loved one and check they've asked for this money.

Find out how to stay safe from scams on our Fraud Hub.'

Lloyds contacted the beneficiary bank to attempt to recover Mr B's money, but unfortunately no funds remained in the account.

Mr B disagreed with Lloyds so brought the complaint to our service. One of our investigators considered the case and didn't uphold it – he thought that, in the circumstances, Mr B ought to have taken further steps to confirm the legitimacy of the messages before making the payment. He also thought that Lloyds didn't need to provide an effective warning at the time of payment, as the scam risk wouldn't have been apparent to Lloyds. The investigator therefore didn't consider that Lloyds needed to do anything to put things right for Mr B.

Mr B didn't agree with the investigator. To summarise, he considered he had done enough to identify that it was his daughter contacting him. He said that considering his age and not being tech savvy, he was more vulnerable to internet scams and that as Lloyds is clearly aware of this particular scam, it could do more to prevent these incidents and protect customers.

As Mr B disagreed with the investigator's opinion, the complaint has been passed to me for 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.

Having done so, while I'm sorry to disappoint Mr B, I'm not upholding his complaint. I'll explain why.

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.

When thinking about what is fair and reasonable in this case, I've considered whether Lloyds should have reimbursed Mr B under the provisions of the CRM Code and whether it ought to have done more to protect Mr B from the possibility of financial harm from fraud.

There's no dispute here that Mr B was tricked into making the payment. He thought he was making a genuine payment to a family member and that didn't happen. But this isn't enough, in and of itself, for Mr B to receive a refund under the CRM Code. The Code places a level of care on Mr B too.

The CRM Code

As I've mentioned, Lloyds is a signatory 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 and it is for Lloyds to establish that a customer failed to meet 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 what the CRM Code refers to as an "Effective Warning" by failing to take appropriate action in response to such an effective 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

**Further exceptions outlined in the CRM Code do not apply to this case.*

I think Lloyds has been able to establish that it may choose not to fully reimburse Mr B under the terms of the CRM Code. I'm persuaded one of the listed exceptions to reimbursement under the provisions of the CRM Code applies.

Taking into account all of the circumstances of this case, including the characteristics of the customer and the complexity of the scam, I think the concerns Lloyds has raised about the legitimacy of the transaction Mr B was making are enough to support its position that he didn't have a reasonable basis for believing the person he transacted with was legitimate. I'll explain why.

I wholly appreciate that Mr B was unaware of this type of scam and was therefore not alive to the possibility it could be a scam when receiving the initial messages. However, having reviewed Mr B's testimony, both to us throughout his complaint and when raising the scam by telephone with Lloyds, I think Mr B did have suspicions about the legitimacy of the messages by the time he made the payment. I say this because Mr B tried to call the fraudster before sending the funds, and within the messages has confirmed this was to check it *was* his daughter. He then called his daughter's landline straight after the payment was sent, despite having been told she wasn't at home as he's explained he was 'doubtful' and 'wanted to check' she was in. I think Mr B's actions demonstrate he wasn't entirely convinced by the fraudster, but still chose to proceed. When Mr B did call his daughter's landline and confirmed she was in, the 'spell' of the scam was immediately broken. I think it's therefore fair to say that had Mr B followed these suspicions prior to making the payment, the scam wouldn't have been successful.

I've also considered the warning Lloyds provided at the time Mr B made the payment. The warning is solely relevant to the type of scam Mr B fell victim to. Mr B confirmed in his call with Lloyds that he saw a warning that mentioned something about fraud and read it, but was convinced it was his daughter he was speaking to. Again I think if Mr B had followed the advice provided in Lloyds' warning, based on his ability to contact his daughter straight after the scam, this would've prevented the scam from happening.

Mr B has also mentioned that he was suspicious when entering the payee's details as he'd assumed that if he was paying an invoice, he must be paying a business account. However, he then received a notification that while the account details were correct, it was a personal account. Mr B has acknowledged that he didn't think that sounded quite right, as companies don't usually deal with personal accounts.

I've also considered that Mr B had received a (seemingly unrelated) other scam text ten days prior to the one he fell victim to, which appears he thought was also from his daughter. That message confirmed the 'daughter' was getting a new phone that day. This therefore doesn't tie in fully with the story Mr B then received from the fraudster that, ten days later, his daughter's phone was frozen for 48 hours due to a phone number change. The fraudster's story was also inconsistent at times, advising Mr B that her phone wouldn't turn on, but was then texting him on what appeared to be the 'messed up' phone. While these inconsistencies

on their own are quite minor in the wider picture, I think they become more relevant when combined with the fact that Mr B already had some suspicions.

I appreciate that Mr B made some efforts to confirm it was his daughter, and was reassured when she described his appearance – however, this conversation took place after Mr B had already made the payment to the fraudster, so I can't fairly say this influenced his basis for belief at the time of making the payment. I also understand Mr B has said the messages had his daughter's name at the top of the screen. However, I think it's more likely than not that this was because Mr B saved the fraudster's telephone number at the beginning of the scam, even though he may not have recalled doing so. I say this because, from our understanding of this scam, fraudsters will contact a lot of people at random, in the hope that some may respond – but won't usually have any information about the people they're contacting. I think if the fraudster knew Mr B's daughter's name, they would have used it to their advantage by making reference to it – to make the scam more believable. In addition, the first message the fraudster sends Mr B asks him to save the number and he replies 'OK'. I therefore think this is why the name appeared this way on his phone screen.

With all of the above in mind, in the particular circumstances of this case, I consider that Mr B ought to have had concerns about the legitimacy of the messages he'd received and this, in turn, ought to have led to a greater degree of checking on Mr B's part. In not carrying out sufficient checks I don't find he had a reasonable basis for believing he was speaking with his daughter and so fell below the level of care expected of him under the CRM Code.

Should Lloyds have done more to try to prevent the scam and protect Mr B?

I've thought about whether Lloyds did enough to protect Mr B from financial harm.

The CRM Code says that where firms identify APP scam risks in a payment journey, they should provide Effective Warnings to their customers. The Code also says that the assessment of whether a firm has met a standard or not should involve consideration of whether compliance with that standard would have had a material effect on preventing the scam.

I am also mindful that when Mr B made this payment, Lloyds should fairly and reasonably also have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). I appreciate that Mr B also feels that, as Lloyds has a clear awareness of this scam, it should be doing more to protect its customers under the Code and ensuring payments being made are legitimate.

Having considered the payment Mr B made, I don't think it was so remarkable, in comparison to his usual account activity, that it should've appeared as suspicious to Lloyds. I therefore don't think Lloyds failed to meet its standards under the Code by not providing Mr B with an effective warning, prior to processing the payment (although it did nevertheless provide a warning related to this scam type).

Whilst I understand Mr B's strength of feeling that Lloyds should protect customers from known scams, I think it's also important to remember that, in this case, Lloyds *didn't* know Mr B was making a scam payment. Lloyds provided a warning relevant to the scam based on Mr B confirming it was a payment being made to family or friends, but, of course, the majority of payments individuals make to family and friends *aren't* scam payments. Therefore Lloyds does have to strike a balance between protecting its customers and also allowing its customers to send money efficiently with minimal disruption. Based on the value of this payment, I think the warning message Lloyds provided online was a sufficient level of 'intervention' and don't consider it was required to take further steps, prior to processing the payment.

Once it was made aware of the scam, Lloyds tried to recover Mr B's funds, but unfortunately was advised by the beneficiary bank that no funds remained. I understand why Mr B would feel frustrated by this, as I can see he had to make a number of calls to Lloyds for his claim

to be logged. While I don't doubt this would've added to Mr B's stresses and frustrations at an already difficult time, I don't think this had any impact on Lloyds' ability to recover Mr B's funds. I say this because the receiving bank has confirmed the account in question was emptied in less than half an hour after Mr B made the payment, which was before Mr B had made his first call to Lloyds. I therefore don't think Lloyds could reasonably have recovered Mr B's payments, even if there hadn't been issues with its phone lines. Lloyds has provided Mr B with £50 compensation to apologise for the difficulties he had logging his fraud claim, and for delays receiving an answer to the claim. I think this is fair to reflect the additional, unnecessary stress Mr B experienced.

Overall, I'm satisfied that Lloyds' position on Mr B's fraud claim, and its assessment under the CRM Code, is fair and reasonable in all of the circumstances and that Lloyds shouldn't be held liable for Mr B's losses. And so I don't intend to make an award to Mr B.

I do sympathise with Mr B as he's clearly been the victim of a cruel scam. But the circumstances of the case and the evidence available lead me to find I'm unable to uphold this complaint.

My final decision

My final decision is that I do not uphold Mr B's complaint against Lloyds Bank PLC.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 21 February 2024.

Kirsty Upton
Ombudsman