DRN-3681021

The complaint

Ms K is unhappy that Lloyds Bank PLC ("Lloyds") hasn't refunded her in full after she was the victim of a scam.

What happened

In May 2021 Ms K was contacted by scammers claiming to be from her internet provider. She'd been expecting a call from this company as she'd reported poor service. The scammers told Ms K she was experiencing poor service because hackers were accessing her network and trying to access her bank accounts. The scammer convinced Ms K to download software which gave them access to her device.

The next day the scammers called again and said she needed to go into branch and remove £20,000 from her account. She says the scammers had manipulated her account to make it look as though an additional £20,000 had been credited so she didn't think she was removing her own money. They told her she needed to withdraw £20,000 in cash in branch and pay this back to the account it came from – the scammers account. The scammers told Ms K she would need to lie to bank staff about what the money was for because she was involved in a high level operation to catch the hackers that were targeting her.

When Ms K went into branch she was questioned by staff about the payment and told them the money was for a family member in financial difficulty. Staff went through a checklist asking her several questions about the payments and providing warnings about fraud and scams but she continued with the payment. After this, the scammers continued to ask Ms K to move money from her accounts and she recognised the situation was a scam.

Ms K contacted Lloyds but it didn't feel it was responsible for her loss. She brought the complaint to our service and our investigator upheld the complaint in part. They didn't think Ms K had a reasonable basis for believing what the scammers had told her, but they also didn't think Lloyds had evidenced she'd ignored any effective warnings in this case.

Lloyds accepted the investigator's findings but Ms K didn't. She felt she was acting reasonably in accepting what she'd been told by scammers. 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.

Lloyds 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 Lloyds 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, and;
- 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.

Did Ms K ignore an effective warning?

Lloyds has said it did provide Ms K with an effective warning in this case. And I think it ought to have given one due to the size of the transaction Ms K was carrying out. When she made the withdrawal in branch it asked her the questions outlined on a standard checklist used with high value transactions. It's said this warning was effective as defined by the CRM code but having considered it carefully I don't agree.

I think Ms K was asked a number of questions that related to her circumstances broadly and I think the conversation as whole ought to have impacted her belief in what the scammers had told her and I've said more about this below. But overall I don't think the warning was impactful due to the amount of different scams talked about and the amount of questions she was asked which largely seemed to be around who she claimed she was sending the money to and why. And, although Lloyds has said the conversation specifically involved telling Ms K her internet provider won't ask her to move money, I haven't seen sufficient evidence this is the case as this isn't what the checklist provided says.

Overall, as I don't think the warning can be defined as effective under the code I don't think this exception applies.

Did Ms K have a reasonable basis for believing the scammers?

I've considered very carefully what Ms K has said about the scam itself. In particular her strength of feeling that the manner in which the scammers explained the situation to her was convincing, particularly as she felt she didn't have a good knowledge of what techniques they could use on her computer to convince her. But overall I don't think she had a

reasonable basis for believing what the scammers told her. In reaching this conclusion I've taken the following into account:

- Ms K has said scammers told her that £20,000 had been deposited into one of her bank accounts. It's not clear if she thought this was deposited by hackers who were targeting her money or by the people who were trying to catch the hackers. It's also not clear what reasons were given for why this had been done. She was then asked to go into branch and move the money in person as this would help her internet provider catch the hackers. I understand the scammers were likely quite persuasive, but I don't think Ms K has been able to provide any plausible explanation that explains why she would need to do this or how it helped her internet provider catch online criminals they said they knew the identity of. Even if it was plausible she was helping with a high level investigation, I think it ought to have stood out to her as concerning she was being asked to move money herself in order to try and catch someone else who was reportedly trying to steal her money.

- Ms K accepted the scammers story that they were involved in a high level fraud investigation with her bank. It's not clear to me why she thought her internet provider would be working to protect her bank accounts. But, I think it ought to have concerned her that throughout this story she was told she wasn't allowed to speak to her actual bank at any point. I think it ought to have seemed even more concerning to her that she was then told she needed to lie to her bank when she withdrew money from her account.

- Ms K has said she's received lots of 'phishing' emails in the past regarding cryptocurrency and from reliable sources that informed her that her details had been compromised and this added to her belief in what the scammers had told her. In particular she's mentioned an email from her insurance provider which she says informed her that a policy had been taken out in her name without her knowledge. We've asked Ms K for evidence of the emails she's said corroborated the scammers' story and added to her belief in the scam, but she hasn't provided these.

- Whilst I don't think Lloyds provided an effective warning as defined by the CRM code, Ms K had a lengthy conversation with someone in branch about fraud and scams where the details of the type of scam she'd fallen victim to were essentially explain to her. She was asked if she'd been asked to move money and was told no organisation would ask her to do this. She was asked, within the context of scam warnings, whether she'd been asked to download anything, let anyone take control of her computer and if she'd been told to move money she'd been overpaid. I think this conversation, together with the other points I've mentioned above ought to have impacted Ms K's belief in what she thought she was doing.

- After Ms K gave the scammers access to her device, they manipulated her screen to make it appear as though money had been transferred to her account. And I accept this is a sophisticated measure and understand why she found this persuasive. But, according to the information she provided to the bank when she reported the scam, the scammers told her there would be a delay in this money showing on her balance. It's not clear whether Ms K was given a plausible explanation for this and it seems at

odds with how direct transfers generally work. I think it would've been reasonable for Ms K to have checked her balance when she was at the bank or before she withdrew the money to try and verify this credit given how unusual the circumstances were and given the other concerning factors I've mentioned above. Or, if she believed the money would be added to her balance after she'd carried out the transfer, it's not clear why she couldn't wait until the money appeared if she was helping with an investigation.

Ms K has said she thinks she did have a reasonable basis for belief, and much of this seems related to the skill of the scammers to socially engineer her. Essentially their manner and the conversational techniques they used whilst speaking to her. And I have taken into account that scammers are very good and very convincing when speaking to their victims as a starting point. But I'd also expect a reasonable person to look for confirmation of what they're being told before moving large amounts of money to a strange bank account.

Ms K has expressed several times that throughout her interactions with the scammers she did have concerns and did ask them to verify what they were telling her. She asked to speak to more senior people and was provided with false staff numbers. But I don't think these things reasonably ought to have reassured her given the magnitude of what she was being asked to do.

I'd also point out that this scam took place across several days. And whilst I accept there was a degree of pressure and urgency placed upon her, I think this fell away overnight after the first scam call. The scammers didn't ask her to move money until the following day. I think this gave her time to reflect on what she was being told away from the scammers influence.

I've considered whether or not Lloyds did enough to try and recall the funds from the receiving bank once it was alerted to the scam. I can see it did contact the receiving bank in this case straight away and according to its records the response received was that the funds could not be returned. There's nothing more I would've expected Lloyds to do in this case.

Putting things right

Lloyds is liable for 50% of Ms K's loss. It should reimburse her for this (£10,000) plus interest.

It appears that £15,000 came from another account Ms K held with Lloyds. So interest should be payable on £7,500 at the account rate (or at 8% if a current account). Interest on the remaining £2,500 should be paid at a rate of 8% as this money was in her current account.

Interest should be paid from 9 July 2022, when Lloyds answered the complaint and ought to have refunded her loss, until the date of settlement.

My final decision

I uphold this complaint and require Lloyds Bank PLC to pay the settlement I've outlined above. Under the rules of the Financial Ombudsman Service, I'm required to ask Ms K to accept or reject my decision before 30 September 2022.

Faye Brownhill
Ombudsman