DRN-4517251

Complaint

Mrs K is unhappy that Lloyds Bank PLC 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 here. What follows is a summary of the key events.

In March 2023, Mrs K fell victim to a safe account scam. She received a text message from a third-party payment provider. It said *"Due to an unusual login we have suspended your account. To unsuspend your account visit [hyperlink]."* Mrs K followed the link and said she was taken to a screen which contained her personal details, including her home address and her date of birth. It asked her to click a link to confirm her identity. However, she paused to think and was concerned about the possibility that the message wasn't legitimate, so she didn't do so.

In the days that followed, there was an attempt to contact Lloyds about Mrs K's account, but the caller failed to pass security checks. Lloyds asked her to get in touch by phone. She did so and it was confirmed that the text message she'd received was likely part of a scam. Her debit card and internet banking was suspended. During that phone call, the call handler at the bank said the following to Mrs K:

> *"We are just going to let you know we will never personally call you, we will never call you on any future dates asking you to move funds to a safe account. We don't do that, so if you get a phone call from anyone saying they are from the bank or the fraud team, it's highly likely it'll be a scam, so if we need to contact you, it'll always be via text message, unless you've arranged a call back with us."*

The employee of the bank clarified whether Mrs K had taken any steps other than clicking on that initial link – i.e. whether she had volunteered any more information to the scammers. She confirmed that she hadn't. A few moments later in the call, the call handler speculated about what the fraudsters were attempting to do by saying that *"they phish for your details …. That's the start of it, then they try and call the bank to phish for more details thinking that, by speaking to us, a colleague's going to perhaps give more information away…"*

The following day, Mrs K received a phone call from someone who claimed to be working for the Financial Conduct Authority. They said they were working alongside Lloyds and carrying out fraud prevention work. They told her that her money wasn't safe in her account and that it needed to be moved to a safe account. Unfortunately, the caller was a fraudster. She says that she did challenge the caller about being asked to move her money. She was told that, while she wouldn't normally be asked to do so, these circumstances were different. She was told that the fraudsters had near immediate access to her funds. I understand this was also the reason why she was told not to end her call with the FCA and call the bank instead. She was told that someone was attempting to make transactions from her account at that precise moment.

Mrs K says that she also asked the fraudster to prove their authenticity by asking them to

confirm her current account balance and her last transaction. She says that the fraudster was able to answer those questions accurately. The fraudster also apparently knew that she'd had a conversation with Lloyds about attempted fraud the previous day. This persuaded her that she was genuinely speaking to someone working with the bank.

She made three payments of £100, £19,000 and £95 respectively. She then attempted to make a fourth payment of £17,995 but this was blocked by the bank for fraud checks. It was at this point that Mrs K recognised that she must have fallen victim to a scam. She made these payments to accounts held by named individuals, rather than accounts in her own name. She was told that this was necessary because her own account was being monitored and it would make it harder for the scammers to target an account that wasn't in her name.

The second of those payments (the £19,000 one) prompted Lloyds to present the following warning message during the payment process:

> *"Just a minute.*
>
> *Be sure that you know who you're sending money to. Please check the account details with a trusted source.*
>
> *Fraudsters invent persuasive reasons to get you to make a payment. See all the latest scams fraudsters use on our fraud hub page.*
>
> *Failure to take precautions before you make your payment could mean we are not able to get your money back in the event of fraud."*

Mrs K voluntarily proceeded past the warning and made the payments. Once she realised she'd fallen victim to a scam, Mrs K complained to Lloyds. In particular, she complained about the apparent ease with which the scammers were able to obtain information about her account that was subsequently used to trick her into thinking she was genuinely speaking to someone working with her bank.

Lloyds didn't uphold her complaint. It considered her complaint under the terms of the Lending Standard's Boards Contingent Reimbursement Model (CRM) Code. It didn't think it was required to reimburse Mrs K under that code. It said it had done everything it could to protect Mrs K. In particular, it cited the warning it had given to her during the call the previous day. The complaints handler wrote:

> *I don't feel you've done enough to protect yourself. You've challenged the caller throughout your conversation but have done nothing to validate them and have just taken their word for everything. We also told you we would never call you and ask you to move money out of your account the day before and you told us you understood this.*

Mrs K was unhappy with the response she received from Lloyds and so she referred her complaint to this service. It was looked at by an Investigator who upheld it. Lloyds disagreed with the Investigator's view and so 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 broad terms, the starting position at law is that a firm is expected to process payments

and that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account.

However, that isn't the end of the story. Lloyds is a signatory to the Lending Standards Board's Contingent Reimbursement Model Code ("the CRM code"). This code requires firms to reimburse customers who have been the victim of authorised push payment ("APP") scams, like the one Mrs K fell victim to, in all but a limited number of circumstances.

Under the CRM Code, a firm may choose not to reimburse a customer if it can establish that:

- The customer ignored an effective warning in relation to the payment being made; or

- In all the circumstances at the time of the payment, in particular the characteristics of the Customer and the complexity and sophistication of the APP scam, 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.[1]

I've considered each exception separately below.

The warnings

For Lloyds to rely on the first exception, the warnings it gave must meet the criteria set out in the Code. Those say that, as a minimum, effective warnings should be:

> *(i) Understandable – in plain language, intelligible and meaningful to the Customer*
>
> *(ii) Clear - in line with fair, clear and not misleading standard as set out in Principle 7 of the FCA's Principles for Businesses*
>
> *(iii) Impactful – to positively affect Customer decision-making in a manner whereby the likelihood of an APP scam succeeding is reduced. This should include steps to ensure that the Customer can reasonably understand the consequences of continuing with an irrevocable payment;*
>
> *(iv) Timely – given at points in the Payment Journey most likely to have impact on the Customer's decision-making;*
>
> *(v) Specific – tailored to the customer type and the APP scam risk identified by analytics during the Payment Journey, and/or during contact with the Customer.*

I'm satisfied that the system generated warning that was displayed to Mrs K during the payment journey wasn't an effective warning, as defined in the Code. The Code says that, where possible, warnings should be tailored to the relevant scam type. Mrs K had been targeted by a safe account scam, but the content of that warning didn't address that particular risk.

Lloyds has also sought to rely on the warning it gave during the conversation with Mrs K the day before the scam happened. I've considered its arguments on this point carefully, but I

[1] There are further exceptions within the CRM code, but they don't apply here.

still think the verbal warning fell short of the criteria set out above. Specifically, I don't think it was sufficiently impactful. I'll explain why.

It is true that Mrs K was told that the bank wouldn't call her and tell her to move her money to a safe account. Unfortunately, this wasn't elaborated upon. She wasn't told that a fraudster would most likely tell her that the safety of her funds was compromised, that she needed to act urgently or that there was a risk that there was an employee of the bank involved. The verbal warning she was given could, in my view, only really be sufficiently impactful if Mrs K already knew what a safe account scam was. I don't think it can be taken for granted that there is widespread public knowledge about how such scams take place.

Unfortunately, the call handler muddied the waters a little by speculating about what the fraudster had been trying to accomplish. The explanation suggested that the fraudsters wanted to obtain her personal information so that they could impersonate her in interactions with the bank. It wasn't explained to her that it's a common scam technique to persuade victims to think that something has compromised the security of the account first and then attempt to protect them from that risk by proposing they put their money in a safe account. This is consistent with what Mrs K has said. She didn't think that, if scammers were able to steal her money, they would do so by socially engineering her to make the transfers herself.

As I've found that neither warning met the criteria set out above, it follows that I don't find that Lloyds can rely on that exception to reimbursement here.

Did Mrs K have a reasonable basis of belief?

Under the CRM Code, if a customer makes a payment with a reasonable basis for believing they're doing so in connection with a legitimate request, the firm should reimburse that customer. I've considered the facts of this case carefully and I'm satisfied that Mrs K *did* act reasonably here. She'd been primed to think that she'd been targeted by fraudsters following the suspicious text message and attempted call to the bank. When she received a call that significantly raised the stakes, she was inevitably more receptive to what she was told.

She also didn't simply accept at face value that the call had come from the bank. She was clearly mindful of the background fraud risk and so wanted to check the legitimacy of the caller. The fraudster was able to confirm information about the account that (as far as Mrs K was concerned) only the bank could've known. This persuaded her that the call had genuinely come from someone working with Lloyds.

The subsequent potential "red flags" must be seen in that context. For example, I understand Mrs K was sceptical about being asked to make payments to an account that wasn't in her name. She was given an explanation as to why this was necessary which I think she was only inclined to believe because she'd already accepted that the caller was genuine.

I've also taken into consideration that the call she had with Lloyds the previous day. I won't repeat the observations I've already made about that call above, but it clearly prompted her to take greater care when the fraudsters contacted her. It was on that basis that she challenged them in the way that she tells me she did. But I don't think the contents of that call put her in a position where she could've known that the follow-up call could only have been from a fraudster. As a result, I don't think the contents of that conversation were such that she made these subsequent payments without a reasonable basis for believing they were being made in connection with a legitimate purpose.

Overall, I'm satisfied that Mrs K's sincere belief was reasonable and, in similar circumstances, the reasonable person would've responded in the way that she did. As a result, I don't find that Lloyds can rely on this exception to reimbursement.

Final decision

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

If Mrs K accepts my decision, Lloyds Bank PLC should refund the money she lost to the scam, less the amount that was recovered from the receiving accounts. It should also add 8% simple interest to that sum calculated to run from the date it declined her claim under the CRM Code until the date any settlement is paid.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs K to accept or reject my decision before 23 May 2024.

James Kimmitt
Ombudsman