DRN-5006163

Complaint

Mr and Mrs A complain that Lloyds Bank PLC didn't do more to protect them when they were targeted by a fraudster. Although this is a joint complaint, the fraudster mainly interacted with Mrs A and so I've tended to refer to her throughout the text of this decision.

Background

The background to this case is lengthy and complex. I haven't set it out comprehensively here, but I have referred to everything that I consider relevant to the outcome I'm proposing.

On 3 February 2021, Mrs A was contacted by someone who claimed to be an employee of Lloyds working in their fraud team. She was told that there had been evidence of suspicious activity on her account and so she was being referred to a specialist team at the Financial Conduct Authority ('FCA'). The people she spoke to at the 'FCA' told her that they were part of a team responsible for conducting investigations into potential fraud by bank employees. The people who had contacted her were not genuine employees of these organisations, but scammers. In this section of my decision, I will refer to the scammers as 'the FCA' or the 'FCA agents', as that was how they presented to Mrs A.

I understand Mrs A was sceptical at first, so the 'FCA' agent suggested she look up the phone number for the FCA online. She saw that it matched the number she was being called on. She wasn't aware that it was possible to spoof numbers in this way and so she was reassured that the call was likely genuine.

The scam took place against the backdrop of the coronavirus lockdown. The scammers used that to support their story. They told Mrs A that, since lockdown, banking regulations for bank staff had *"gone out of the window"* due to staff working from home. This had led to internal fraud at Lloyds and other financial institutions.

Mrs A was told that the security of her own accounts had been compromised by specific Lloyds employees who were under investigation. Her money was therefore at risk. It needed to be moved to safety as quickly as possible. Over several weeks, they were able to persuade Mrs A to part with over £475,000. These payments were made from her accounts with Lloyds.

Mrs A felt that, as the 'FCA' were dealing with the matter, it must be serious. That made her feel very anxious. The 'FCA' told her two agents had been assigned to her case. Those agents asked her to work with them to help catch the fraudsters. Once sufficient evidence to support a prosecution had been obtained, they said the case would be passed to the police and arrests would be made.

Mrs A recalls the 'FCA' agents appeared to be working tirelessly and over long hours on her behalf. She recalls asking them if they ever went home. They told her they'd get a week off once the investigation was complete. She was given a password that needed to be shared each time she spoke with them. She was told this would change each week to ensure security. Mrs A also recalls the 'FCA' agents always called her when they said they would. She felt supported and well looked after during a time which she says she felt lonely and

isolated due to lockdown restrictions.

The ‘FCA’ told Mrs A her accounts at Lloyds, an account with another bank, and an account held with an investment firm were all at risk. They told Mrs A that, in order for them to catch the Lloyds’ employees and to ensure her money was safe, she’d need to make transfers from her account with Lloyds into a new account they’d set up for her. They told her she needed to move her money via her account with Lloyds because they’d taken out insurance with a well-known firm to cover Mrs A’s funds in the event of any losses, should anything go wrong. The insurer would only cover one account. Mrs A received an assessment of her account risk profile, as well as a letter explaining the insurance the ‘FCA’ had taken out on her behalf. Both documents were sent on FCA headed paper.

In addition, the ‘FCA’ told Mrs A it had set up a Club Lloyds account in her name and that the ‘FCA’ had put in £330,000 which would also cover any losses should anything go wrong. Mrs A received a spoofed Club Lloyds statement in her name, c/o the FCA. The ‘FCA’ told Mrs A that to compensate her for her time and help she would receive 4.4% of the funds she was due to move –approximately £20,000 in total. Mrs A says she found the demeanour of the ‘FCA’ agents, and the steps they’d apparently put in place to protect her, to be consistent with what she’d have expected from an organisation investigating large scale fraud.

On 7 February, Mrs A says that the ‘FCA’ agents told her the urgency of the situation had increased. Lloyds staff had attempted to make a payment to a bank account in Dubai. This payment had been attempted without “second stage sign-off”. They told her that this meant a senior employee at Lloyds was involved. Mrs A asked to see evidence of the payment attempt and was sent a SWIFT Transfer Request Form. It appeared to show that, in 2 days’ time, a payment of £349,000 would be made to a bank account in Dubai. The ‘FCA’ told her they had the power to delay the payment and that would give them enough time to move her money to safety. Mrs A says the ‘FCA’ added to her already anxious state by explaining the insurance they’d taken out to protect her didn’t cover international payments. She therefore needed to act quickly and move her funds to safety. They told her she had two weeks to move all her money as they’d put a ‘two-week delay’ on the payment transfer.

Mrs A recalls being concerned this ‘delay’ would cause suspicion with the individuals at the bank who were alleged to be involved. The ‘FCA’ reassured her that banking staff were used to payments sometimes taking up to two weeks and so they had plenty of time to move her money to safety as well as gather enough evidence of internal fraud to present to the police. Mrs A recalls believing the ‘FCA’ would operate in this way.

A new account was created by the scammers with a third-party business, that I’ll refer to as L. L is a firm that operates a cryptocurrency exchange. The ‘FCA’ told Mrs A the account with L was in her name – which it was. Mrs A said this ‘terrified’ her. She did not want to buy Bitcoin and knew nothing about cryptocurrency. The ‘FCA’ told her not to worry as the money would sit in her ‘wallet’ at L. No cryptocurrency would be purchased. They explained it was merely a holding measure and supported her in downloading an ‘app’ to access her account. Mrs A was ultimately persuaded the money was ‘safe’ given the account was in her name and, on the face of it, she had control of it.

Her first payment to this account was for £1,000 and this went through unchallenged. The ‘FCA’ encouraged her to make this small payment first so that she could check that money had been safely received by an account in her name. Once she was satisfied this was the case, Mrs A was prepared to move the rest of her money to safety.

The ‘FCA’ told Mrs A to visit her local Lloyds branch and request a payment to her L account for £375,000. Mrs A recalls the ‘FCA’ briefed her on all the questions she’d be asked in branch and told her to “stay strong” in the face of any resistance. She recalls the ‘FCA’

evoked urgency by being forceful with their instructions, repeating them several times. The 'FCA' agents told her that it was critically important that she not reveal to any employee of the bank that she was being asked to do this by the 'FCA' or the investigation would be compromised. They also told her to leave her mobile phone on in branch. This would allow the 'FCA' to gather evidence about who the corrupt employees were.

Mrs A recalls Lloyds staff noticed she was on the phone when she asked to make the payment and told her to turn her phone off. She does not recall them explaining the significance of this, although a later disclaimer she signed (which I'll set out in full later in this decision) suggests otherwise. She told the bank she was transferring the funds because she wanted to invest in cryptocurrency. Mrs A recalls being asked whether she was certain 'L' was reliable. As far as the other questions were concerned, she was able to give the answers that had been provided to her by the 'FCA' agents.

Mrs A says she was given a leaflet detailing commonly occurring fraud scenarios. She says bank staff didn't talk her through the leaflet, but she doesn't recall its content referring to internal fraud, the impersonation of FCA employees or moving money to a customer's own account. She also says that the bank employee wanted to show her a video about scams but couldn't load it on her computer. She was told that she'd have to go to a different branch if she wanted to go ahead with the payment. On reporting back to the 'FCA', Mrs A was told that this employee was a subject of the investigation, and that Mrs A shouldn't trust them.

She says this created a feeling of outrage in her against the bank. The 'FCA' agents once again prepped Mrs A for a branch visit. They even told her Lloyds might call the police to establish she knew what she was doing. She visited the other branch and asked it to transfer £330,000 to the third-party account. A bank employee went through the same steps as had taken place at the other branch and Mrs A says she was shown the video. However, the employee said that she wouldn't make the transfer until Mrs A had spoken with a member of the Lloyds fraud team.

Mrs A recalls waiting for some time to speak to the fraud team, with a member of Lloyds branch staff. After a little while the branch staff member said she had to go and make a phone call and would be back soon. Mrs A was suspicious that, perhaps, the employee had gone to speak to an accomplice. She returned with the name and number of a member of Lloyds' fraud team but unfortunately this made Mrs A more suspicious that she'd end up speaking with someone implicated in the investigation. At this point, Mrs A said she trusted no one at Lloyds.

She was put on the phone to an individual in the Lloyds fraud team. Mrs A described his approach within this conversation as *"aggressive"* – I cannot say whether that is a fair description because there isn't a recording of the phone call available. In any case, the result of the call was that Lloyds invoked the Banking Protocol – an arrangement between banks and the police under which a police officer will visit the branch and, if necessary and appropriate, attempt to break the spell a customer is under.

Mrs A told the branch staff that she couldn't wait for a police officer to arrive. The fraudsters had, in any case, told her that she must not under any circumstances tell the police what was going on. The investigation was hanging in the balance and doing so might tip off the fraudsters at Lloyds. I understand she was visited at home that evening by a police officer.

From Mrs A's description, the enquiries by the police officer seem to have focussed on whether she had the capacity to manage her own money, rather than attempting to deal with the concerns Lloyds had about her being targeted by scammers. She says she had a brief conversation with the police officer about what she was making the payment for and whether she was doing it of her own volition. The police officer was satisfied with her answers and

said he would tell the branch. However, that officer didn't report back, so Mrs A's payment wasn't processed. No record of the conversation is available.

At the insistence of the 'FCA', Mrs A went to the branch the following day and attempted to make the payment again. Lloyds contacted the police once more. An officer visited the branch and spoke with Mrs A. As with the prior interaction, Mrs A says the police officer didn't have any concerns.

Nonetheless, Lloyds didn't go ahead with the payment because it still had concerns about the fraud risk. Mrs A emailed Lloyds to show it evidence that the third-party account was in her name and that the earlier deposit of £1,000 was still in her e-wallet. On 12 February, the member of the Lloyds fraud team contacted Mrs A and said that, to go ahead with the payment she'd need to sign a disclaimer. The disclaimer was worded as follows:

> *We are writing in connection with your request to make a CHAPS payment of £330,000 to [L] from your Lloyds Bank account … We believe there is a high likelihood that this could be a scam. We first received this request from you in [Branch A] on 8 February. We were concerned that you were on the phone while in branch and have advised you that this is often seen in scams. We wanted to show you some educational videos however due to issues with getting them to load and as your parking ticket was about to expire you left the branch before we could do this.*
>
> *You then attempted to make the payment later that day from [Branch B]. After asking you questions about the investment our branch colleagues were suspicious that this could be a scam and so we asked [the] Police to come to branch under the Banking Protocol, however, they were unable to attend before you left. We understand that the Police did visit you at home to discuss the payment.*
>
> *The following day you attempted to make the payment in [Branch B]. We again invoked Banking Protocol and you spoke to a Police officer in branch, however, as we remained suspicious we declined to make the payment. You then also tried to send £25,000 via online banking on the evening of 9th February however this flagged on our systems due to high risk of fraud and was not processed.*
>
> *We have advised you that [L] is not regulated by the Financial Conduct Authority ('FCA') and that in January 2021 the 'FCA' issued the following notice for consumers wishing to invest in crypto assets, which include Bitcoin:*
>
> *"Investing in crypto assets, or investments and lending linked to them, generally involves taking very high risks with investors' money. If consumers invest in these types of products, they should be prepared to lose their money".*
>
> *We have also advised you that several other of our customers have reported fraud against the account details where you are attempting to send your money, and that much of what you have told us about your interactions with [L] has the hallmarks of a scam.*
>
> *We have advised you that criminals impersonate the Police, Banks' Fraud Departments, the National Crime Agency, HMRC and other trusted organisations.*
>
> *They may already know some of your personal or banking details and use this to convince you they are genuine, before urging you to move your money to keep it safe, and/or to liquidate existing investment products. The funds are then sent to an account controlled by the criminals, even though they might have told you it is held in your name. It is common in these types of scams for investors to be shown their*

funds and profits via online portals - these are fake.

We request that you acknowledge receipt of this letter and confirm that you:

- *Have chosen to invest with [L] of your own free will and not under duress or the instruction of any third party.*
- *Understand the advice that Lloyds Banking Group has given you about scams and that we remain concerned you may become the victim of fraud.*
- *Understand and accept the risks associated with this and any future connected transactions.*
- *Understand and accept that Lloyds Banking Group will not refund you in the event your investment transpires to be a scam.*

Lloyds' system notes from 13 February suggest it found evidence of remote-access technology being used to access Mrs A's online banking, so it suspended it. On 15 February, Mrs A signed the disclaimer. The same day internal notes from Lloyds suggest it had concerns she had fallen victim to an investment scam. Mrs A says she (and Mr A, having spoken to the 'agents' to check their legitimacy himself) remained completely certain that they were dealing with the 'FCA'. Her online banking access was reinstated, and she was able to authorise the £330,000 payment.

It's not entirely clear why, but the payment was returned to Mrs A's account. She says the 'FCA' told her that the payment had been recalled by the Lloyds employee she'd spoken to on the phone. They told her that this employee had recalled the payment because he too was under investigation. She was told that the Lloyds employee clearly wanted the money to stay in her current account so that he could make the international payment. The 'FCA' told Mrs A they'd managed to intercept messages sent between two employees of the Lloyds fraud team, one of which was a member of staff Mrs A had spoken to. The 'FCA' shared an extract from a WhatsApp conversation between the 'bank employees' which showed them conspiring to defraud Mrs A with messages such as *"We keep stalling her - do you think she's on to us?"* and *"I'm trying to put this international payment through."*

Ultimately, the £330,000 payment wasn't processed. Undeterred, Mrs A started to transfer funds in smaller sums. Several of these payments triggered a response from Lloyds' fraud team and she had to call them before the payments could be processed. Mrs A recalls it was difficult to get hold of Lloyds by phone to get these payments processed. This was in contrast with her experience dealing with the 'FCA' agents who were always on hand to support her. In total, Mrs A was able to transfer just over £475,000 to the account with L.

Mrs A realised she'd fallen victim to a scam after discussing what had happened with her son. She notified Lloyds right away. It said it wouldn't refund her losses. In its final response, it said *"because the payments were made to a [third-party] cryptocurrency account in your name which you had control of at the time, this scam and investigation must be completed by [L]."* The investment provider, however, refunded the money she lost from her investment.

Mrs A wasn't happy with Lloyds' response and so she referred her complaint to this service. It was looked at by an Investigator who didn't uphold it. The Investigator thought Lloyds had done everything it could reasonably have done in the circumstances. It had invoked the Banking Protocol twice. However, that course of action is no guarantee that potential fraud will be uncovered. Lloyds had no control or influence over the questions asked by the individual police officers who attended.

The Investigator thought that, even if Lloyds had handled things differently, Mrs A could not have been talked out of going ahead with the payments. Her belief that she was protecting her own savings and aiding law enforcement authorities was simply too entrenched. He also

thought that there were several potential red flags that should've been a cause for concern and made her question whether the proposal she was going along with was a legitimate one.

The Investigator didn't consider the case against the provisions of the Lending Standards Board's Contingent Reimbursement Model Code ("the CRM Code"). He said that Mr and Mrs A's losses weren't covered by the CRM Code because the payments from the Lloyd's account were made to another account that was controlled by Mrs A. He said that meant it fell outside of the scope of the CRM Code.

Mrs A responded to the Investigator at length. The crux of her argument was that the bank's fraud prevention systems could only have been effective if Mrs A continued to trust bank staff. The fraudsters were able to make it exceptionally difficult for any employee of the bank to establish that trust. A friend of Mr and Mrs A also thought the payments should be considered under the CRM Code. Since Mrs A disagreed with the Investigator's opinion, the case was passed to me to consider.

Findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I issued a provisional decision on this complaint on 6 August 2024. I wrote:

> *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 2017 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 CRM Code. The CRM Code requires firms to reimburse customers who have been the victim of authorised push payment ("APP") scams, like the one Mrs A fell victim to, in all but a limited number of circumstances.*
>
> *Lloyds responded to Mr and Mrs A's complaint by saying that the CRM Code didn't apply because she paid an account in her own name. When the case was looked at by the Investigator, he came to broadly the same conclusion about the applicability of the code. I've given the facts of this case careful consideration, and I'm not persuaded that this is the case.*
>
> *The CRM Code defines an APP scam in the following way:*
>
> *a transfer of funds executed across Faster Payments, CHAPS or an internal book transfer, authorised by a Customer in accordance with regulation 67 of the PSRs, where*
>
> *(i) The Customer intended to transfer funds to another person, but was instead deceived into transferring the funds to a different person; or*
> *(ii) The Customer transferred funds to another person for what they believed were legitimate purposes but which were in fact fraudulent.*
>
> *It is not disputed that Mrs A transferred funds for what she believed were legitimate purposes, but which were in fact fraudulent. The key question for the purpose of determining whether the payments Mrs A made from her Lloyds accounts fall within the scope of the CRM Code is whether she transferred those funds to "another person."*

In April 2023, the Lending Standards Board wrote to CRM Code signatories (including Lloyds) to provide a clarificatory update on this point. This document set out three scenarios that it considered did fall within the scope of the CRM Code. This is one of those scenarios:

> *"An account was opened by or for the customer as a result of social engineering by the scammer. The customer then credits the account at the direction of the scammer in the belief that those funds are secure (for instance, as part of a safe account scam) but the scammer has access to those funds (whether or not the customer is aware). If the customer has been socially engineered, the customer may believe the scammer has a legitimate reason to be able to access their crypto asset account or may have unknowingly shared sufficient details with the scammer to allow them to access the account. In such cases, the customer has, in effect, made a payment to another person for what they believed to be a legitimate purpose, and they have lost control of the funds at the point at which they are transferred to the crypto exchange."*

This is comparable to what happened in Mrs A's case. As I understand it, the account with L was in Mrs A's name and, although she didn't open the account herself, she did have access to it and so did the scammers. She said she was told it had been opened for her and the scammers gave her a password to use when she downloaded the app. She had access to the account, to the extent that she was able to show an employee of the bank her e-wallet to persuade them that they shouldn't obstruct her in making the payments.

Mrs A retained a theoretical measure of control because she could have moved the funds back to the originating account, but to all intents and purposes, the money was under the effective control of the fraudsters once she'd transferred it to the third-party account. That enabled the fraudsters to move the funds on without her knowledge which was always their intention.

For the reasons I have described, I'm satisfied that Mrs A transferred funds to another person for what she believed were legitimate purposes, but which were in fact fraudulent and that the payments therefore do fall within the scope of the CRM Code.

<u>Should Lloyds have reimbursed Mrs A under the provisions of the CRM Code?</u>

The starting point under the CRM Code is that signatory firms should refund customers who are victims of APP scams. However, the Code says that firms can opt to not reimburse a customer if it can establish that one of the exceptions to reimbursement applies.

The relevant exceptions are:

- *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: (i) the payee was the person the Customer was expecting to pay; (ii) the payment was for genuine goods or services; and/or (iii) the person or business with whom they transacted was legitimate.*

- *The Customer ignored Effective Warnings, given by a Firm in compliance with SF1(2), by failing to take appropriate action in response to such an Effective*

Warning…[1]

I've taken into account whether the first exception to reimbursement applies. Lloyds doesn't have to reimburse Mrs A if she made these payments without having a reasonable basis for believing that they were part of an authentic law enforcement operation. It's worth noting at the outset that the way this test is framed in the CRM Code is not entirely objective. There is a specific provision that allows me to take into account "the characteristics of the Customer".

While some customers might respond to what Mrs A was told with scepticism, I have to bear in mind the extent of Mrs A's knowledge of financial products and services which, by her own admission isn't extensive, as well as her circumstances at the time.

Taking all of that into account, I'm persuaded that her belief that these payments were made in connection with a legitimate purpose was a reasonable one. Although scams have grown exponentially in terms of their complexity in recent years, the scam that Mrs A fell victim to was particularly complex and sophisticated in terms of the detail, the lengths the scammers went to establish credibility, and the extent of the social engineering they undertook. Several critical steps were taken in the earliest stages to get Mrs A to buy in to the notion that these requests were legitimate. This included number spoofing (something she wasn't aware was possible) and sending a copy of a "risk assessment" that looked very much like it could've been an official document produced by the FCA.

The scammers also supplied Mrs A with an altered bank statement. This showed a Lloyds bank account which appeared to be in her name, but had "c/o the 'FCA'" in the first line of the address. The statements made it look as if a six-figure sum had been deposited into that account for insurance purposes. The false narrative that was created by the scammers – i.e., that a small group of employees of the bank were conspiring to steal customer money – was supported by what appeared to be plausible documentation, such as the SWIFT transfer form and the intercepted messages between two employees of the bank.

The faked message exchange was consistent with the fact that Mrs A had been told the fraud investigator she spoke to on the phone was a target of the investigation. As I explained above, Mrs A told us that she found the tone of that employee to be aggressive. Unfortunately, Lloyds hasn't been able to provide a recording of the call that might help me to understand if that's a fair assessment. It's worth noting that, if that was a fair characterisation of that phone call, it can only have made it easier for the scammers to persuade Mrs A that employee was being investigated and was being difficult for that very reason.

There was a vacuum of information here which the scammers sought to fill. This allowed them to set the terms of all her interactions with genuine employees of the bank further down the line. I accept that Lloyds recognised the serious risk of fraud here and took extensive steps to protect Mrs A. I've looked at the disclaimer which it asked her to sign before any payments would be processed. This very bluntly sets out the concerns the bank had, although not all were relevant to the scam Mrs A was falling victim to. From the bank's perspective, there were several possible scam types that might have targeted her. Account notes suggest the bank was most concerned Mrs A had fallen victim to an investment scam (which might explain why, in her submissions, she has appeared to take less notice of the warnings about other

[1] There are other exceptions, but they aren't applicable in this case.

scams). In practice, given what Lloyds knew, it couldn't have been more precise in the content of its warning unless Mrs A shared more detail about why she was making the payments. That was extremely unlikely to happen given what she'd been told by the scammers.

I am satisfied the scammers were able to engender a sense of distrust towards employees of the bank who were there to protect her from financial harm. As a result, the impact of the written disclaimer and the verbal explanations given to her were greatly reduced.

I've also considered whether the two visits from police officers ought to have undermined Mrs A's belief in the scam. Unfortunately, there are no records of the conversations that took place. Mrs A recalls both officers concluded that she sounded like she knew what she was doing and had the capacity to make financial decisions. I find Mrs A's account plausible. Nevertheless, I don't doubt that visits from the police are rare or extraordinary events and this might have prompted Mrs A to take note of Lloyds, rather than the scammers. I've thought carefully about this. Since the scammers had primed Mrs A to expect a visit from the police, coupled with what appears to have been lack of scam warnings delivered by the officers, those visits, in essence, became far less impactful.

I've also considered the time frame in which these events took place. However, rather than providing Mrs A with breathing room, the delays allowed the scammers to establish a strong relationship with Mrs A over and above the relationship the bank could establish. That meant she was utterly convinced by what she'd been led to believe – that is, that she was helping a fraud investigation balanced against the need to protect her money over a lengthy and draining period. Overall, I think Mrs A did have a reasonable basis for belief here.

I've also considered whether the second exception regarding 'effective warnings' is applicable here. To reach a finding on this point, I must consider:

- *Whether the warnings given by Lloyds to Mrs A were "effective warnings" in compliance with requirements of the CRM Code set out at SF1(2).*
- *If they were, whether Mrs A ignored those warnings by failing to take appropriate action in response to them.*
- *Finally, if so, whether taking appropriate action would've had a material impact on preventing the scam that went on to take place.*

If it can't be demonstrated that each of these requirements has been met, then the exception to reimbursement does not apply under the provisions of the CRM Code.

SF1(2) says:

"Where Firms identify APP scam risks in a Payment Journey, they should take reasonable steps to provide their Customers with Effective Warnings, which should include appropriate actions for those Customers to take to protect themselves from APP scams.

a) Firms should take reasonable steps to make their Customers aware of general actions that could be taken to reduce the risk of falling victim to an APP scam
b) Where the Firm identifies an APP scam risk, it should provide Effective Warnings to customers. This may occur in one or more of the following:
    i. when setting up a new payee

ii. when amending an existing payee; and/or
iii. during the Payment Journey, including immediately before the Customer authorises the payment, before the Customer's account is debited.

c) Effective Warnings should be risk based and, where possible, tailored to the APP scam risk indicators and any specific APP scam types identified through the user interface with which the Customer is initiating the payment instructions.

d) Effective Warnings should enable the Customer to understand what actions they need to take to address the risk, such as more appropriate payment methods which may have additional protections, and the consequences of not doing so.

e) As a minimum, Effective Warnings should meet the following criteria:
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, under the CRM Code, whether a warning is effective in compliance with SF1(2) will depend upon the following:

- *It must as a minimum meet the UCITS criteria (understandable, clear, impactful timely and specific) set out above. As these are minimum criteria, it may be necessary for the warning to do more than just meet the UCITS requirements to amount to an effective warning – it would not be an effective warning if the information provided did not give the customer a better chance to protect themselves against being defrauded.*

- *It should include appropriate actions for customers to take to protect themselves from APP scams and they should enable customers to understand what actions they need to take to address the risk of APP fraud, such as more appropriate payment methods which may have additional protections and the consequences of not doing so.*

It is unfortunate that Lloyds hasn't been able to provide contemporaneous evidence of all the warnings it gave Mrs A – including notes of discussions in branch as well as some of the call recordings. But in reaching my conclusions as to whether the effective warning exception should apply in this case, I have considered the various interventions from Lloyds that I do have evidence of. This includes the scam leaflet, a video, the disclaimer Mr and Mrs A signed as well as a call recording Lloyds has shared. And even in the absence of contemporaneous evidence of the other interventions Lloyds provided, I've still thought carefully about the cumulative effect of all the intervention communications Mrs A received.

Turning to whether the warnings Lloyds gave Mrs A were effective, this isn't a straightforward question to address. I have considered the position carefully against the expectations set out at SF1(2). There is no doubt in my mind that Lloyds went to great lengths to protect Mrs A from financial harm from fraud. Mrs A has highlighted a number of things that Lloyds could've done differently, such as talk her through the scam leaflet, or provide detail in its warnings that more closely aligned with the scam she fell victim to. I don't agree that Lloyds needed to be more specific in its warnings based on the information available to it.

Nonetheless, based on the evidence I've seen, I think Lloyds could've provided better warnings or warnings that strictly met the definition of an 'effective warning' in the CRM Code. But taking into account the volume of warnings, the time period over which they were given, the number of payments that were declined and the cumulative effective of all of these factors, I don't think I can safely conclude that Lloyds did not provide Mrs A with effective warnings.

I've therefore gone on to consider the second element of the effective warning test – whether Mrs A ignored the effective warnings Lloyds provided by failing to take appropriate action in response to these warnings. The question posed by the reimbursement section of the CRM Code is whether the customer ignored an effective warning by failing to take "appropriate action" in response. The way the effective warning criteria is drafted means that a warning does not necessarily need to respond to every feature or nuance of a scam in order to comply with SF1(2). This reflects the fact that the 'effective warning' requirements are found in the standards for firms and are prevention measures that firms are expected to take to reduce the occurrence of APP scams by giving customers information to help them protect themselves.

And whilst the list of minimum requirements includes criteria that requires some connection between the warning and the particular scam type to be effective, it is possible that a particular feature of a scam will render a warning that meets the SF1(2) criteria ineffective in practice, depending on the individual consumer and the circumstances. This means a customer might reasonably continue with a payment, notwithstanding the warning they have been given.

Given the background and context to this reimbursement exception and the over-arching principle that lies behind the CRM Code (i.e. that the customer should be reimbursed except where they fail to meet their requisite level of care) I'm satisfied that in considering whether the customer ignored an effective warning by failing to take appropriate action in response to it, it is necessary to take into account the particular circumstances of the scam and the customer, and what action (or lack of) it would have been reasonable for a customer to take in those circumstances. In other words, appropriate action means considering whether the customer failed to act reasonably in response to the warning.

I'm also mindful the Practitioner Guide to the CRM Code explained that in deciding not to reimburse a customer because the customer ignored an effective warning , firms should have regard to the characteristics of the customer and the complexity and sophistication of the APP scam in determining whether it would have been reasonable for the Customer to undertake the actions identified in the warning.

I have considered whether Mrs A failed to take appropriate action in response to the warnings she received given the particular circumstances of the APP scam she fell victim to. I understand she was given a leaflet when she initially went into branch to attempt to make payment. I don't know what was said in branch. Mrs A's and Lloyd's submissions on this are somewhat contradictory. But I do have a copy of the leaflet Mrs A was given. She has stressed the branch staff did not talk her through the leaflet and feels they should have done.

She recalls 'reading' the leaflet but because of her state of mind at the time, she says she did not digest the contents. And on reflection Mrs A doesn't feel the contents as written were specific enough to have 'broken the spell'.

The leaflet sets out six of the most commonly occurring scam types in a table. The first of those scams was described in the following way:

> *"Fraudsters can call pretending to be a bank, the police, well-known companies or organisations. They can copy telephone numbers so they look genuine."*
>
> *"Fraudsters want you to move money to another account. To get you to do this, they'll say things like:*
>
> - *There's a problem with your account.*
> - *They need your help to catch criminals.*
> - *The bank are trying to steal your money or are issuing fake notes.*
> - *You owe money to HMRC.*
>
> *They may scare or threaten you to do as they say. And tell you to keep it a secret."*
>
> *<u>How to avoid the scam</u>*
>
> *If you get a call like this, hang up. If you're in branch, tell the staff and they'll help you."*

I am satisfied that this wording is understandable and clear. It's directly relevant to the scam that had targeted Mrs A and, if she'd read and absorbed the contents of the leaflet and properly thought about them, I think it could've meaningfully affected her belief in the legitimacy of the request.

But Mrs A wasn't 'reading' this leaflet in the cold light of day. She has repeatedly and consistently shared that she was feeling incredibly anxious throughout the period she was interacting with the scammers. That level of anxiety can impair the ability to take on board information, in many formats, and reduces the scope for rational reflection and thought. Mrs A says she was handed the leaflet, but that its contents weren't discussed with her and there's no evidence to suggest that it was – for example, in the form of notes recorded on her account or customer profile. I would expect an employee of the bank to have talked her through the information contained in the leaflet, otherwise its impact would be reduced.

Mrs A recalls the conversation that took place in branch focused on the risks associated with investing in cryptocurrency. I find that plausible given that Lloyds' internal notes also state they're concerned Mrs A was falling victim to an investment scam. I am also mindful that the scammers had manipulated Mrs A not to trust Lloyds' staff.

Against that backdrop, I can understand why the content of the leaflet didn't resonate with Mrs A. Overall I do not think Mrs A failed to take appropriate action in response to the leaflet given its limitations and circumstances in which it was given to her.

<u>The video</u>

Lloyds has shared two videos with us. It appears a customer can self-select one or the other. It's not clear which Mrs A would've seen at the time. I've spoken to her about her recollections. She says she recalls a video that featured an elderly man who'd fallen victim to an investment scam. The video content she describes doesn't correspond with either video that Lloyds has shared with me. I'm therefore not persuaded I can safely conclude the

videos Lloyds has provided were the videos Mrs A was shown at the time. Mrs A has, in any event, stressed that it's important to remember her state of mind at the time.

Nonetheless, I have considered the possibility that Mrs A saw both videos at the time. However, given the extensive social engineering she'd been subject to and her state of mind, it's more likely than not that she wouldn't have processed their contents, which is plausible given that her recollections aren't consistent with the videos Lloyds shared with me.

The written disclaimer

Mrs A signed a written disclaimer following Lloyds' ongoing concerns that she'd fallen victim to a scam. The full text is reproduced in the background section of this decision.

It's noteworthy that SF1(2) requires an effective warning to include "appropriate actions for … Customers to take to protect themselves from APP scams." The text of the disclaimer didn't include any content that covered what steps Mrs A ought to take to protect herself, though I accept it's implicit that Mrs A shouldn't proceed with the payment. Nonetheless, it was fairly unambiguous in communicating that Lloyds believed Mrs A to be falling victim to a scam. So as above, I've considered whether Mrs A (and Mr A given he co-signed it) failed to act reasonably in response to the warnings contained within the disclaimer by making the payments.

I accept Mrs A's representations that she, unfortunately, put no weight on the information provided by Lloyds because she had complete distrust in them – this distrust had built over time and was particularly pronounced at this point following the tactics of the scammers. Mrs

A has said the disclaimer didn't warn her about scammers using stories of internal fraud or the impersonation of fraud investigators working for the FCA. I also think it is more likely than not that Mrs A did, as she says, take a great deal of comfort from the fact that the money was in her account with L. As a result, she never thought she was at risk of harm from fraud. I also accept her representations (taking into account the extent of the social engineering she had been subject to) that the lack of information addressing this specific factor meant it didn't resonate with her. I'm also satisfied that Mr A too believed this was a genuine law enforcement operation too after having one phone conversation with the fraudsters to check the legitimacy of the situation.

I'm sympathetic to the difficulties Lloyds had in preventing the scam here. It cannot cover every single detail of each possible scam type in a way that would resonate with every individual customer. That is not expected of firms under the CRM Code. But customer reimbursement under the CRM Code is not based on whether a firm could've prevented a scam – where exceptions to reimbursement don't apply, firms are expected to reimburse customers even where there is 'no blame' on either side.

In this instance, I'm persuaded the disclaimer simply came too late to have the necessary impact, and I say that even having taken into account that Mrs A had several days to think about its contents. Mrs A has said she felt acute stress by this point. Her only objective was to move her money to safety. By the point she was asked to sign the disclaimer, she'd already been told by the scammer that the fraud team member she'd spoken to was a target of the investigation and been shown the fake messages exchanged between two Lloyds employees. In the particular circumstances of this case, there was a very limited prospect of the disclaimer serving as a warning and preventing her from going ahead with the payments.

It's difficult to understand why Mrs A would have gone ahead with all the transactions if she had any doubt as to whether what she was doing was legitimate.

While I have taken into account how strongly worded the disclaimer was, taking into account the circumstances in which it was presented and the level of social engineering Mrs A was subject to, I don't think Mr and Mrs A acted unreasonably to the extent that I can find they failed to take appropriate action in response to the disclaimer.

Even after Mrs A signed the disclaimer Lloyds still intervened and warned Mrs A ahead of processing payments on three occasions. Only one of these calls is still available. I've listened to this but here the warnings were generic, lacked impact and don't meet the definition of an effective warning under the CRM Code. That's not to say I think better warnings at this stage would've made a difference.

Whilst Lloyds hasn't been able to evidence all the interventions it made in its efforts to protect Mrs A from financial harm from fraud, I'm persuaded these interventions took place. Given the number of warnings Lloyds gave and the number of times it refused to process Mrs A's payment requests, I've considered the cumulative effect of all of the interventions and warnings Mrs A received and whether she ought to have responded differently to them.

Mrs A has given a detailed and compelling account of the psychological manipulation and social engineering she was subjected to, how the coronavirus lockdown restrictions had a role to play, and how she was completely taken in by the fraudsters given the relationship they built with her and the sense of support they provided. It's unfortunate, but understandable to some extent, that her experience of dealing with Lloyds staff played into the scammers story. Of course, Lloyds staff weren't in a position to build such strong ties as the scammers had with Mrs A. Unfortunately, the level of sophistication of the scam meant that the multitude of interactions and warnings from Lloyds were insufficient to overcome the strength and sophistication of the scam and break the spell Mrs A was under.

In the circumstances and given how the scam unfolded, I do not think Mr and Mrs A acted unreasonably so as to fail to take appropriate action in response to the warnings they were given, particularly when taking into account the sophistication of the scam.

Was Mrs A vulnerable?

Finally, Mrs A has said she was vulnerable at the time the scam occurred. A customer is vulnerable to APP scams if it would not be reasonable to expect that customer to have protected themselves, at the time of becoming victim to an APP scam, against that particular APP scam. In these circumstances, the customer should be reimbursed notwithstanding the exceptions to reimbursement noted within the Code.

Mrs A has referred to the lockdown restrictions imposed by the government in response to the coronavirus pandemic and the feelings of isolation associated with this. She's referred to the fear and uncertainty that was felt across the whole country at the time. In addition, because she was regarded as clinically vulnerable, the scammers compounded the fear she was already feeling at the time. She's explained that this fear and anxiety she felt reduced her scope for rational thought.

I've no doubt that the pandemic played a role here. It's clear from Mrs A's submissions that the fraudsters used what was a significant global event to underpin their story of internal bank fraud and it was a time where it felt as though anything was possible. I think the pandemic was a relevant factor that contributed towards how Mrs A was feeling at the time.

That is one factor that contributes to my finding that Mrs A did have a reasonable basis for belief that what she was doing was legitimate. But I don't find Mrs A was vulnerable based on the definition outlined above – in other words, I don't think she was unable to protect herself from the scam due to vulnerability. Instead, I think Mrs A was unable to see the

fraudsters for what they were due to the level of sophistication they deployed. It's for similar reasons that Lloyds was very unfortunately unable to break the spell too.

Conclusions

For the reasons set out above, I am satisfied that the CRM Code does apply to the circumstances of the payments Mrs A made. And having considered the reimbursement provisions of the CRM Code and the limited exceptions to reimbursement, I am satisfied that Mr and Mrs A are entitled to be reimbursed for the payments made.

As I have explained, it would have been difficult for Lloyds to have done more to warn Mrs A about the possibility she might be the victim of a scam. But the reimbursement provisions of the CRM Code are not focussed on whether the firm could have done more to prevent the scam succeeding, but instead on whether an exception to reimbursement applies.

For the reasons I have set out above I am not persuaded an exception to reimbursement applies in this case. I'm therefore satisfied Lloyds should fairly and reasonably have reimbursed Mr and Mrs A, notwithstanding the action it took to prevent the fraud.

Fair compensation

This is a provisional decision and only sets out what I'm minded to do based on the evidence I've seen. I will consider any further representations from either side before reaching a final decision.

However, I am currently minded to uphold this complaint and direct Lloyds Bank PLC to compensate Mr and Mrs A by doing the following:

- *Refunding the payments they made in connection with the scam, less the £97,000 that was refunded by the third-party investment firm.*

- *Paying interest on that sum. The funds Mr and Mrs A lost to the scam originated in a savings account held with a different bank. Lloyds should add interest calculated using the rate applicable to that savings account.*

If either party has any concerns about the conclusions I've come to regarding redress, they should let me know in response to this provisional decision.

The rules that apply to this service allow me to award fair compensation to be paid of up to £355,000 plus any interest that I think is appropriate. A final decision along these lines will mean that the compensation is above that limit.

I intend to recommend that Lloyds pays the balance. That recommendation is not part of my determination or award. Lloyds wouldn't have to do what I recommend. In the event that the final decision is along these lines, if Lloyds doesn't intend to pay the balance above the award limit, it should let me know in its response to this provisional decision.

It's unlikely that Mr and Mrs A could accept a final decision and go to court to ask for the balance. They may want to get independent legal advice before deciding whether to accept this decision.

Responses to the provisional decision

Mrs A responded to say that she accepted the provisional decision. Lloyds didn't agree. It raised three specific points. First, it pointed out that branch staff had gone through its high-

value checklist with her. This standard document included a verbal warning which branch staff were instructed to read to the customer. That verbal warning includes text pointing out that fraudsters *"may contact you by, telephone, knocking on your door or via social media. Often fraudsters claim to be from trusted organisations such as Police, HMRC, FCA, your Broadband Company or the Bank's fraud team …"* It says that, as this warning made reference to fraudsters impersonating employees of the FCA, it ought to have resonated with Mrs A and affected her decision making.

Second, it pointed out that Mrs A had said that the FCA agents would, once they had gathered sufficient evidence, hand over the file to the police to make arrests. It questioned why she wasn't willing, therefore, to disclose to the police officer who visited her at home what she'd been asked to do.

Finally, it said that, as well as asking Mrs A to sign the disclaimer before agreeing to remove the restrictions on her account, it also sent her a copy by post the same day. It says that this should've allowed her the opportunity to make sense of its contents in her own time

I've considered these points carefully and, having done so, I'm not persuaded to depart from the findings I set out in my provisional decision. I'll explain my reasons why.

I accept that it would've been the standard process for branch staff to read out the warning from the *'high-value checklist'*. This did include a reference to fraudsters impersonating the FCA. Having said that, I've not seen any specific evidence showing that the process was followed here. Lloyds hasn't provided a copy of the actual form used in Mrs A's case and there aren't any contemporaneous records of its completion or any evidence that bank staff verbally provided information to Mrs A on FCA impersonation scams. That weakens Lloyds' argument that Mrs A should've acted differently in the light of its contents. That said, I do accept it's possible Mrs A was talked through the contents of that document at the time.

However, as I explained in detail in my provisional decision, the interventions provided by Lloyds need to be considered against the backdrop of a highly sophisticated scam, which included an extensive degree of social engineering. In the provisional decision, when discussing the significance of the fraud leaflet, I noted that Mrs A read it, but didn't meaningfully process its contents. This was because she'd been primed to not trust the bank and was also affected by the stress of the situation. If the text on the high-value checklist had been read out to her, I think it's more likely than not that the same thing would've occurred.

I've also considered the fact that Mrs A didn't disclose what she was doing to the police officer who came to visit her. It's been suggested that, since Mrs A thought that the police would ultimately be informed about everything, she shouldn't have had any concerns about telling that specific police officer. I've thought carefully about this, but overall, and considering the particular circumstances of this case, I understand why Mrs A acted in the way that she did. The police isn't a single entity and it would be quite plausible for a fraud investigation to be the responsibility of a different department or a different force. She was tricked into trusting someone she believed was a law enforcement professional. However, it doesn't necessarily follow that she'd be expected to trust any individual police officer. The fraudsters had floated the possibility that the local police might not be trustworthy and told her that this investigation was *"hanging in the balance."* In the circumstances, having developed this connection with the fraudsters, I can understand why she acted as she did.

I've also considered Lloyds' comments about the fact that the disclaimer was posted to her. Lloyds has argued that this would've given her extra time to reflect on its contents. I'm not persuaded that this affects the outcome here. I had carefully considered the length of time Mr and Mrs A had to sign this disclaimer when I reached my provisional findings. By the

point the disclaimer was shared with her, she'd already been conditioned to not trust the bank. I would also reiterate the observations I made in the provisional decision about the period over which these events took place. The delay allowed the fraudsters to cement their relationship with Mrs A. Instead of giving her the necessary headspace to reflect on the actions she was taking, it created a vacuum of information that the fraudsters were able to fill.

I do think it would've been exceptionally difficult for Lloyds to have prevented Mrs A from falling victim to the scam. It clearly recognised the fraud risk here and took multiple steps in its attempt to protect her from it. Nonetheless, the provisions of the CRM Code don't only apply where a firm is at fault for failing to prevent a scam from taking place. Lloyds should've reimbursed Mr and Mrs A under the CRM Code unless an exception to reimbursement applied. For the reasons I've discussed above, I'm not persuaded that's the case here and so Lloyds should fairly and reasonably have reimbursed Mr and Mrs A.

Final decision

Where I uphold a complaint, I can award fair compensation to be paid by a financial business of up to £355,000 plus any interest that I consider appropriate. If I think that fair compensation is more than that limit, I may recommend that the business pays the balance.

Decision and award: I uphold the complaint. I think that fair compensation is £428,964. My decision is that Lloyds Bank PLC should pay Mr and Mrs A £355,000. It also needs to pay interest on that sum using the rate applicable to the savings account from which the funds originated.

Recommendation: Fair compensation is more than £355,000 so I recommend that Lloyds Bank PLC pays Mr and Mrs A the balance of £73,964. I also recommend it adds interest to that sum using the rate applicable to the savings account from which the funds originated.

This recommendation is not part of my determination or award. Lloyds Bank PLC doesn't have to do what I recommend. It's unlikely that Mr and Mrs A can accept my decision and go to court to ask for the balance. They may want to get independent legal advice before deciding whether to accept this decision.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A and Mrs A to accept or reject my decision before 20 November 2024.

James Kimmitt
Ombudsman