DRN-3764942

The complaint

Mr S is unhappy that Lloyds Bank PLC won't refund money he lost as a result of a scam.

What happened

Mr S was searching for an investment opportunity online. He says that he left his details on the website of a well-known price comparison company and subsequently received a call back from whom he believed was an agent of that website. It was recommended that he purchase a bond in the investment arm of a high street bank (that I'll call B).

He called the number he was given and spoke to someone that I'll call M. M said that a 7-year bond at 2% interest would be suitable and that the investment would be fully protected by the FSCS.

Mr S says that after this call he conducted thorough due diligence. He'd been the victim of a very similar scam two years before and, I presume, wanted to ensure that he did not fall foul of the same experience. A complaint about Lloyds' refusal to refund his losses from the previous scam was referred to our service, but the complaint wasn't upheld.

Mr S says he undertook significant due diligence before going ahead with the investment, including:

- Reviewing the company's website.
- Checking the FCA registration of the company.
- Researching M, as well as other individuals he subsequently spoke to.

He also says that he called B on the telephone number listed on the FCA website and asked to speak to M. M wasn't available but, he says, he received a call back from M shortly afterwards. Mr S claims that M appeared aware of the earlier call and reassured him about the investment.

After receiving further documentation from M setting out the details of the bond and sending his identity documents, supposedly for anti-money laundering purposes, Mr S agreed to invest.

He made a series of payments to two different accounts:

13 May 2021 - £9,527.40
14 May 2021 – £19,897.60
20 May 2021 – £20,575
Mr S spoke to Lloyds once before the payment on 13 May 2021 and several times before the payment of 20 May 2021. During the call prior to the 13 May 2021 payment, Lloyds provided some advice about scams but Mr S reassured it that he'd carried out significant due diligence prior to going ahead. During one exchange before the final payment, it questioned why he was making a payment for an investment with B, but not paying one of its accounts. When Mr S asked the fraudsters about this he was told that the account he was paying was

held at a subsidiary of B. The payment was cancelled but the fraudster arranged for another account, this time held by B, to be used and the payment was made the following day. After intermittent communication with M and several failed promises to get in touch, Mr S became concerned. He called B and, after eventually managing to speak to the real M, he realised he'd been the victim of a scam.

Lloyds considered the matter under the Lending Standards Board Contingent Reimbursement Model "CRM Code" which requires it signatories, like Lloyds, to reimburse victims of APP scams like this one in all but a limited number of circumstances. Lloyds said that one of those exceptions applied – that Mr S hadn't done enough to protect himself – highlighting the fact he paid accounts in different names to B and didn't check their actual website.

It did think that it could have done more during the calls which took place before the third payment was released, so it offered to refund 50% of that payment - £10,287.50. It was also able to recover £3,097.61 from the bank accounts which received Mr S' money.

The matter was referred to our service and one of our investigators didn't uphold it. They didn't think that Mr S had a reasonable basis for believing that the recipient of his payments was legitimate and he was paying for genuine services. While they thought that Lloyds hadn't met its standards under the CRM Code by failing to provide an 'Effective Warning', they didn't think this would have made a material difference to the outcome as Mr S was confident in the checks he'd carried out. They also thought that a better intervention by Lloyds would not have brought the scam to light for the same reasons.

Mr S didn't agree. He said that he didn't consider himself to be an experienced investor and had taken all the steps that had been recommended by our service after the previous scam. He felt that the investigator's view was based on supposition and that had he been told by Lloyds that there was a strong chance he was being scammed then he would not have gone ahead. He also didn't understand why the investigator hadn't found Lloyds fully responsible, given they had accepted it didn't provide an effective warning.

As no agreement could be reached, the case was passed to me for a final 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.

I'm very sorry to hear about the loss that Mr S suffered here, particularly given his previous experience. But, having reviewed this matter carefully, I don't think Lloyds should do any more to resolve this complaint. It's important to note that I can't know for certain what might or might not have happened, so my role is to decide what I think is more likely than not, taking into account all the available evidence and arguments.

The starting point, both under the Payment Services Regulations 2017, and the terms of Mr S' account is that he, rather than Lloyds, is responsible for payments he's made himself. The CRM Code somewhat changes this position. Lloyds need to show that one of the exceptions applies to decline full reimbursement. If it can show such an exception applies, it still needs to demonstrate that it met its standards as a firm. If it didn't meet those standards and that failure would have had a material impact on preventing the scam, then it may also be partly responsible for the loss. Lloyds also has longstanding obligations to be on the lookout for unusual and out of character activity which might indicate its customer was at risk of financial harm from fraud.

Lloyds argue that Mr S didn't have a reasonable basis for belief in making the payments, so I've first considered this point.

It's important to say that scams of this nature are often sophisticated and that was certainly the case here. The fraudsters have gone to some lengths to impersonate or 'clone' a genuine business. They used an 0800 phone number, had a professional looking website, impersonated genuine bank employees and provided a reasonably substantial amount of paperwork about the 'investment'.

I've taken all of that into account when thinking about the actions Mr S took. In addition, I need to be fair about the standard which I hold Mr S to. He seems to have had some limited experience of investing, but I don't think he was very experienced. And, I've been careful not to examine events simply through the benefit of hindsight or using my own experience in this field.

Notwithstanding the above, I'm struck by the similarities between this scam and the scam that Mr S fell victim to about two years prior. In the 2019 scam Mr S was contacted about investing in a fixed-term bond. He says that he carried out due diligence – including checking Companies House and the FCA register. And, when he realised there might be a problem, he contacted the real investment company who confirmed that he'd been the victim of a scam.

There were some differences between that scam and this one (for example, in 2019 the fraudster did not impersonate a real person). It also seems that Mr S may have done a few more checks this time before going ahead. However, given his prior experience and the remarkable similarities between the two scams, as well as the fact that this was not a situation where Mr S found himself under any significant pressure to invest, I'd have expected him to have been vigilant about the possibility of fraud.

He knew that firms could be cloned, he knew that paperwork could be faked too (as they had been in relation to the previous scam). He knew that people might claim to work for a business but didn't. With this in mind, I'd have expected him to carry out additional checks at every step.

Mr S believes that he left his details on a popular price comparison website. He may have done this, but it's very unlikely that the call he received back came from that website. Mr S has been somewhat inconsistent about the name of the website he visited. But neither of the price comparison websites he mentions offers this kind of bond and neither, as far as I'm aware, do they operate by agents calling customers directly. The real websites only show rates for fixed-rate savings bonds.

A simple online search would have shown that Mr S was not dealing with the real price comparison website and he would have known that anyone impersonating a genuine business should be treated with extreme caution.

Neither did he do anything to establish whether the person he spoke to actually worked for the price comparison website. Again, this would have been quite straightforward to do and isn't an unreasonable suggestion given his previous experience. Once offered the bond, Mr S doesn't appear to have checked the price comparison website to see if it was advertised. Next he was given a telephone number and told it was that of B. But it wasn't and again an online search would have shown that it wasn't. A prudent next step would be to do a simple online search for B, find the product being suggested and call it on the number listed on its website. Instead Mr S called the number he was given. A simple online search of B would have also led him to an entirely different website.

The paperwork I've seen is also far from perfect, it has unusual use of language and is rather shoddily put together.

Though Mr S did carry out checks, these were largely the same as he had done for the previous scam (and they hadn't been able to detect it). As far as I can see, two additional checks were made: a search for the named individual he spoke to and calling B's number as listed on the FCA website.

While I can see that M is a genuine employee of B, he does not have anything like the same job title as M claimed. M appears to be a senior employee of Barclays and I cannot find any mention of the "fixed income team". So, this search alone could not have given too much reassurance.

Turning to the point on which Mr S puts most weight – the call to B's genuine switchboard. While I haven't seen any evidence that this took place, I'd be surprised if he didn't do it given the circumstances. But, I find it a little coincidental that M was able to ring back within an hour. Mr S says that M apologised for missing the call – suggesting he was aware that the call had been made. But I can't see any reasonable way by which M would have known about the call Mr S made. Again, I'd expect Mr S to be on guard here – to have waited for M to have confirmed that he'd been called and to have checked the number which he was called from.

Following his conversation with M, Mr S agreed to make a number of payments totalling £50,000. But he wasn't told to pay B directly, but rather two different companies – neither of which had an obvious relationship to B. It doesn't appear that Mr S did any research into the names of the recipients and simply accepted that they were linked to B. A quick search online for one of the recipients would, I think, have only given Mr S further cause for concern – as it appears to have operated a retail business, possibly related to vaping.

Lloyds told Mr S that one of the banks he was paying was not, as he had been told by the fraudsters, a subsidiary of B. While, as I'll go onto discuss, Lloyds might have done more at this point, the fact he'd been given incorrect information by the fraudsters should have also caused him further concern.

As mentioned, I don't wish to hold Mr S to an unreasonably high standard and yet I would have expected him to be on the lookout for *anything* concerning about the investment opportunity.

Neither would I have expected him to necessarily pick up on everything that I've noticed that wasn't quite right. But he wouldn't have needed to have picked up on everything – just one or two things ought to have been enough to put him off, particularly considering that he spoke to Lloyds a number of times before the payments were made – all of which gave him time to reconsider.

Overall, I think Mr S missed warning signs that, given his previous experience, he should have been alert to and that means that I don't think he had a reasonable basis for belief and Lloyds can fairly rely on one of the exceptions in the CRM Code to decline full reimbursement.

Did Lloyds meet its own obligations?

Under the CRM Code, Lloyds has obligations, of particular relevance here is the obligation to provide an 'Effective Warning' where it identifies a scam risk during a payment journey. When considering any warning given, consideration must be given to whether a warning is likely to have had a material impact on preventing the scam.

As already mentioned, Lloyds also has longstanding obligations to be on the lookout for unusual and out of character transactions to protect customers from financial harm from fraud.

There doesn't appear to be any dispute that both the first and third payments Mr S made were unusual and presented a heightened risk of APP fraud. This is what prompted Lloyds to intervene before both payments were made.

Lloyds says it provided at least one tailored written warning during the scam. That warning said:

[customer's name] make sure this investment is real

- *Deals that look too good can be scams*
- *Do lots of research – good deals don't find you*
- *Use the FCA to check an adviser or company*

I don't think this warning was effective. It fails, for example, to mention the consequences of proceeding with the payment and doesn't contain any information about how to check whether a firm has been cloned.

It was also always unlikely to be effective in Mr S' circumstances. What he was offered wasn't too good to be true – just a 2% return. He believed he'd, and to a significant extent had, carried out plenty of research and also checked with the FCA. So, I don't think this warning was effective.

Mr S would have also seen another, much less specific, warning. I haven't reproduced that in full here, but it wasn't tailored to the scam risk and I'm satisfied it wasn't effective in the circumstances.

Lloyds also provided some warnings about scams in the calls prior to the payments taking place. In the call prior to the 13 May 2021 transaction, Lloyds, among other things, asked him whether he had control of his account with B. This line of questioning wasn't particularly relevant to the circumstances Mr S was in. But Mr S did explain that he'd previously experienced a scam and had taken all necessary steps – including checking the FCA website. Lloyds also asked questions relating to other common scams including how he'd found out about the investment. Again, I don't think anything within this call constituted an effective warning under the CRM – the warnings were quite general and, as noted, weren't always specific to the most obvious scam risk.

But, at this point, given the checks Mr S had carried out, I don't think he would have been deterred by an 'Effective Warning' that was tailored to the risk of cloned investment scams. He believed he was already fully aware of, and had already taken, the steps he needed to take to avoid falling victim to this type of scam, including contacting B on the telephone number on the FCA website. So, I don't think that an effective warning would have had a material impact on preventing the first two payments.

Lloyds did recognise that Mr S was not paying an account in the name of B during the first call, but the account was held at B, so I don't think this fact alone was enough to cause Lloyds sufficient concern and I wouldn't have expected it, based on the risk presented, to have taken additional steps which might have uncovered the scam (such as asking for the contact details and website he'd been given).

As already set out, there were also a number of conversations that took place before the payment on 20 May 2021. During these calls it was identified that Mr S was not paying an account held at B. He went back to the fraudsters to question this and was ultimately given another account to pay.

I agree with the bank that it should have done more during these calls. It identified that the bank Mr S was paying had nothing to do with B and it shouldn't have been reassured by the fact he put through the transaction again to an account held at B. At this point it was aware that he'd been told a material falsehood by the fraudsters and, taking into account it spoke to Mr S for a significant amount of time, it could have taken some of the simple steps I've outlined above (such as checking the website he'd been given). So, despite Mr S doing plenty to reassure Lloyds, given the obvious risk here, I think it could have and should have identified he was likely falling victim to a scam and prevented further loss to Mr S.

But, for the reasons I've already outlined, I think Mr S had a role to play in what happened and that means that I don't find that Lloyds are fully responsible for the last payment. Instead, I think liability should be shared between Mr S and Lloyds. As Lloyds have already refunded half of the final payment, I don't find that it should do anything further to resolve this complaint.

Finally I've considered whether Lloyds did enough to try and recover Mr S' money. It says that it contacted the receiving bank by about 5pm on the day Mr S reported the scam. I can see that Mr S reported the matter at about midday that day. While I think Lloyds could have taken action a little more quickly, I've seen evidence from the receiving bank which shows no action would have made any difference – no transactions left the receiving accounts between Mr S reporting the matter to Lloyds and Lloyds contacting the bank which received his money.

My final decision

For the reasons I've explained, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 24 February 2023.

Rich Drury
Ombudsman