

## **The complaint**

Mr M complains that Lloyds Bank PLC ('Lloyds') won't refund the money he lost when he says he fell victim to a scam.

## **What happened**

Mr M says he was introduced to a company I'll call H in this decision by an individual who built up a relationship with him. H's promotional literature led him to believe it was an established and reputable company that offered loan notes with a 12% return per year. Funds were to be used for property development. Mr M made two payments to H of £10,000, one on 23 August 2019 and the other on 27 November 2019.

Mr M says he became concerned when payments weren't received and there was a lack of correspondence from H. He later learned that H appointed administrators in January 2022 and was distressed to discover the liquidator's report indicated there was no likelihood of investors like himself being repaid. Mr M says that H operated a scam and never intended to provide the promised returns.

Mr M instructed a professional representative who wrote a letter of complaint to Lloyds in June 2023. This letter said Lloyds should reimburse him under the provisions of the Lending Standards Board's Contingent Reimbursement Model Code ('CRM Code') and, in particular, its provisions in respect of vulnerability. This was because Mr M was a senior citizen and an inexperienced investor when he made the payments. Mr M also said Lloyds should pay interest and £1,000 compensation.

Lloyds didn't agree to reimburse Mr M. It said Mr M had made an investment with a legitimate company that had failed. Lloyds went on to say that if new information came to light it would review its position.

Mr M wasn't happy with Lloyds' response and brought a complaint to this service.

## *Our investigation so far*

The investigator who considered this complaint didn't recommend that it be upheld. He said there was insufficient evidence to conclude that H didn't intend to provide the agreed investment or make the returns it set out. This meant that he couldn't ask Lloyds to consider Mr M's complaint under the CRM Code.

Mr M didn't agree with the investigator's findings and asked for a review by an ombudsman, so his complaint has been passed to me to decide. He asked me to review the following points:

- The investigator applied the wrong threshold test for intervention by Lloyds when considering the application of the CRM Code. The investigator said the CRM Code only applies where the payer's payment meets the CRM Code definition of an APP scam. But the threshold test for triggering action by the bank is whether there was an identifiable scam risk at the time the payment was made. Mr M quoted a section of the CRM Code that says, "Firms should take appropriate action to identify Customers and payment authorisations that run a higher risk of being associated with an APP scam". Mr M said that there was an identifiable APP scam risk which Lloyds failed to act on.

- Mr M made two high value payments in a short timeframe. The payments were out of character, especially given Mr M was retired at the time, and were to a new payee. So Lloyds should have recognised a scam risk.
- The investigator failed to give adequate weight to the information provided to demonstrate that H was operating a Ponzi scheme. Too much weight was given to indicators H was running a legitimate business and too little weight to the implausibility of the returns offered and the required cashflow to generate those returns. H would not see a return from a site until it was sold or refinanced but had to pay commission, interest and bonuses in the short term. Mr M said the logical explanation was that H was using new investor funds to make payments to other investors.
- Administrators for H haven't offered any conclusions on the inter group transactions that are being investigated and certainly haven't concluded there was nothing irregular going on.
- H hasn't filed accounts since 2018. The logical inference is that auditors were unable to sign off H's accounts.
- Mr M said the purpose of the genuine business conducted by H was to give the project legitimacy and encourage investment.
- Given the high rates of return offered and the commission paid to introducers, H would have to generate huge returns which make the rates offered implausible. The logical conclusion is that investor funds were used to make payments to other investors.
- Mr M was vulnerable at the time as he was not a sophisticated investor and thought he would get guaranteed returns. On this basis he should be reimbursed under the CRM Code.
- The loss of his funds has had a huge impact on him financially and emotionally.

### **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.

In deciding what's fair and reasonable, I'm required to take into account relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

Whilst I have considered all points raised by Mr M, I will not comment specifically on each one. I also cannot comment on other decisions issued by the Financial Ombudsman Service.

In broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. But there are circumstances when it might be fair and reasonable for a firm to reimburse a customer even when they have authorised a payment.

Lloyds is a signatory to the CRM Code. Under this code, the starting principle is that a firm should reimburse a customer who is the victim of an authorised push payment (APP) scam, except in limited circumstances. But reimbursement under the CRM Code only applies if the definition of an APP scam, as set out in it, is met.

I have considered whether Mr M's claim falls within the scope of the CRM Code, which defines an APP scam as:

*...a transfer of funds executed across Faster Payments...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) *(ii) The Customer transferred funds to another person for what they believed were legitimate purposes but which were in fact fraudulent.*

It is for Mr M to demonstrate that he is victim of an APP scam.

To decide whether Mr M is victim of an APP scam as defined in the CRM Code I have considered:

- The purpose of the payments and whether Mr M thought this purpose was legitimate.
- The purpose the recipient (H) had in mind at the time of the payments, and whether this broadly aligned with what Mr M understood to have been the purpose of the payment.
- Whether there was a significant difference in these purposes, and if so, whether it could be said this was as a result of dishonest deception.

Mr M thought he was investing in a property development company. I haven't seen anything to suggest that he didn't consider this to be a legitimate purpose.

In reaching an answer on what purpose H had in mind, I've considered the wider circumstances surrounding H and any linked businesses. The key information to this case is:

- H completed three different development projects. H also worked on other developments which it then sold to developers when it experienced financial difficulties. The completion of three development projects is strongly indicative of a legitimate business carrying out the activities I would expect of it.  
  
I appreciate that Mr M believes H completed these developments to give the appearance of legitimacy and to draw in investors. But no persuasive evidence has been put forward to make me believe this is the more likely scenario.
- Points raised by Mr M are largely based on assumptions and indicate poor business and financial management but don't go far enough to bring his claim within the scope of the CRM Code. Whilst H may have misrepresented certain information, not filed accounts, and paid high commissions to introducers, there is currently no evidence to say this was done with the intention of scamming investors. A lot of adverse inferences have been drawn here.
- I've not seen anything from the administrators of the company to suggest the company was operating a scam or that the transactions carried out by the company and connected companies were done with any intention other than putting investors' funds towards development projects. Whilst transactions are being investigated, there is currently no evidence that funds weren't used for the intended purpose.
- I also haven't been provided with evidence following an investigation by any other external organisation which concludes that H intended to use Mr M's funds for a different purpose.

Having carefully considered all the evidence provided to me, I'm not persuaded there is sufficient evidence to conclude that the purpose H had in mind when it took Mr M's payment was different to his. So, I consider Lloyds acted fairly in not considering Mr M's complaint under the CRM Code.

If material new evidence comes to light at a later date Mr M can ask Lloyds to reconsider his fraud claim.

Mr M says the investigator misapplied the CRM Code. The CRM Code is clear that subject to certain exceptions a customer "who has been the victim of an APP scam" should be

reimbursed. Likewise, the provisions in respect of reimbursement when a customer is vulnerable apply when, at the time of becoming victim to an APP scam, that customer couldn't have protected themselves from the scam they fell victim to. So, reimbursement under the CRM Code, whether because of vulnerability or because an exception to reimbursement doesn't apply, is dependent on the definition of an APP scam being met.

The code includes other provisions relating to the detection and prevention of scams. Mr M's representative has quoted from the section of the CRM Code that relates to the detection of payment authorisations that run a higher risk of being associated with an APP scam. The section on prevention refers to the warnings customers should be given if a firm identifies an APP scam risk in a payment journey. These provisions tie in with Lloyds' wider obligation to be on the look-out for unusual transactions or other signs that might indicate that its customer was at risk of fraud (among other things). In some circumstances, Lloyds should take additional steps, or make additional checks, or provide additional warnings, before processing a payment.

In this case the payments Mr M made weren't unusual or out of character given his previous account activity. He made two separate £10,000 transactions in March 2019 (one of which related to an investment given the payee name) and a £20,000 payment in May 2019. The two payments to H also weren't in quick succession.

In any event, even if I concluded that Lloyds ought reasonably to have intervened, I'm not persuaded it would have had any concerns, or that the payments would not have been made. H was a legitimate company that at the time the payments were made and was paying returns to other investors. Detailed documentation was provided to Mr M and there was nothing in the public domain at the time to suggest Lloyds should have been concerned that Mr M might be falling victim to a scam. Many of the concerns Mr M has raised have come to light after payments left his account. And it wasn't for Lloyds to analyse in detail the documentation provided to Mr M or to provide investment advice.

I'm very sorry to disappoint Mr M, as I know he has lost a significant amount of money and his health has suffered. But I'm not satisfied that I can fairly ask Lloyds to refund him.

### **My final decision**

For the reasons stated, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 9 December 2024.

Jay Hadfield  
**Ombudsman**