DRN-4186115

The complaint

Mr J complains Lloyds Bank PLC ("Lloyds") won't refund the money he lost as a result of a third part scam.

Mr J is represented by a third party.

What happened

The full details of this complaint are well known to the parties, so I won't repeat them here. Instead, I'll recap the key points, and focus on giving reasons for my decision:

In November 2021, someone contacted Mr J on a social media site about an investment opportunity. The individual - who I will refer to as V - was impersonating a friend of a friend. V told Mr J he could get returns of £5,000 in a week on a £500 investment. He was given access to a trading platform where he could see his investment in real time. When he asked to withdraw his funds, he was asked to pay £2,200 in tax and also a further £1,500 in fees. He then realised he had been the victim of a scam.

Our investigator did not uphold the complaint, she felt the payments weren't unusual and were relatively low in value, so she didn't think Lloyds needed to intervene or provide a warning. She also considered that Mr J did not have a reasonable basis for belief or that Mr J was vulnerable to the extent that he was unable to protect himself.

Mr J did not accept the investigator's conclusions, so the case has been passed to me for a decision.

What I've decided – and why

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

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 terms and conditions of the customer's account. So, although it wasn't his intention to pay money to the scammer, under the Payment Services Regulations 2017 (PSRs) and the terms of his account, Mr J is presumed liable for the loss in the first instance.

However, taking into account the law, regulatory rules and guidance, relevant codes of practice and good industry practice, there are circumstances where it might be appropriate for a bank to take additional steps or make additional checks before processing a payment in order to help protect customers from the possibility of financial harm from fraud.

When thinking about what is fair and reasonable in this case, I've considered whether Lloyds should have reimbursed Mr J in line with the provisions of the Lending Standards Board Contingent Reimbursement Model (the CRM Code) it has signed up to. And whether it ought to have done more to protect Mr J from the possibility of financial harm from fraud.

There's no dispute here that Mr J was tricked into making the payments. He thought he was sending money to an investment and this wasn't the case. But this isn't enough, in itself, for Mr J to receive a full refund of the money under the CRM Code.

The CRM Code

Lloyds has signed up to the CRM Code. The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment (APP) scams like this, in all but a limited number of circumstances.

One such circumstance might be when a customer has ignored an effective warning.

A second circumstance in which a bank might decline a refund is, if it can be demonstrated that the customer made the payments without having 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

There are further exceptions within the CRM Code, but they do not apply in this case.

The CRM Code also outlines the standards a firm is expected to meet. And it says that when assessing whether the firm has met those standards, consideration must be given to whether compliance with those standards would have had a material effect on preventing the APP scam that took place.

I am also mindful that when Mr J made these payments, Lloyds should fairly and reasonably also have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). And in some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

Did Lloyds meet its obligations under the CRM Code and did Mr J ignore an effective warning?

The CRM Code says that 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.

I accept that the first payment of £500 was to a new payee – but the payment was unremarkable and the transfers after that were to the same known payee. The transfers were relatively small (between £500 and £2,200) and spread out, and Mr J had made larger transfers than these in the months prior to the scam. Banks can't reasonably be involved in every transaction. There is a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments. Overall, I don't think the transactions Mr J made stood out as being unusual or that Lloyds ought reasonably to have identified a risk here.

That said, it seems that Lloyds did provide a warning for '*something else*' which is what Mr J told Lloyds he selected at the time the payment was processed. I haven't repeated the warning that was shown during the online payment process because Mr J's choice made it very difficult for Lloyds to give a tailored and impactful warning. It's also the case that, had answering '*investment'* (as arguably he should have done) led to a warning that met the

definition of 'effective' under the CRM Code (that's not a finding I need to make here), it would be irrelevant because Mr J didn't see that particular warning. So, I don't find that Lloyds has failed in its obligation to provide an effective warning, but I also can't say Mr J ignored an effective warning either.

Did Mr J have a reasonable basis for belief, or could Mr J have done more to mitigate his losses?

I need to consider not just whether Mr J believed he was sending money for an investment but whether it was reasonable for him to do so. I've thought about the steps Mr J took to reassure himself about the legitimacy of the transactions and whether it was reasonable for him to proceed with the payments.

I don't agree with Mr J's representative that he had no reason to doubt the legitimacy of the investment and or his dealings with the advisor. I say this because:

- Mr J was told he would receive £5,000 in a week from an investment of £500. The promised returns were unrealistic and too good to be true and the deal warranted closer scrutiny.
- Mr J was asked to pay taxes upfront. I think this ought to have caused concern.
- Mr J came across the opportunity on a social media platform and communication was mainly via a social media messaging platform. No contract or terms and conditions were provided, and he wasn't provided with any clear information on how the funds were invested. This is not how a genuine firm would operate.
- Some messages were sent to Mr J via email and did have documents attached but these communications were not very professional looking.
- The payments were made to a third party in a personal name rather than a business and payee name was unrelated to whom Mr J was corresponding with. I think this was a sign that things were not quite right and should have led to a more cautious approach.

Overall, I don't think Mr J had a reasonable basis for believing these were genuine payments for a genuine investment opportunity or that he was dealing with a genuine person.

Vulnerability under the code

There are provisions under the code which might lead to a refund, even when a customer doesn't have a reasonable basis for belief. The relevant part of the Code, says:

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 of an APP scam, against that particular APP scam, to the extent of the impact they suffered. This should be assessed on a case-by-case basis.

I understand that Mr J was going through a lot and the scam has clearly impacted him further. I note from what his representatives have said, he was dealing with difficult personal circumstances including the loss of a family member and his own father's medical diagnosis. From what's been said, I understand this meant Mr J was under financial pressure as he wanted to ensure that he could cover any fees and/or bills associated with these unfortunate circumstances. Mr J says, if he wasn't under this immense pressure, it is unlikely that he would have fallen victim to this scam.

I'm sorry to hear of all Mr J has been through. Not just in terms of this scam, but also what's happened to him prior to or during the scam. I've no doubt that he has been through a lot and I don't doubt that his mental health has suffered as a result. And no doubt the scam has impacted him further.

But I've considered whether there are vulnerabilities present to such an extent that Mr J was unable to take steps to identify the scam he fell victim to or to recognise steps he might take to test the legitimacy of what he was being told by the fraudster. To do so I must consider the details of the scam, Mr J's actions throughout, and the wider circumstances of what was happening in his life at the time.

Having done so, I consider there is evidence within the circumstances that suggest Mr J was capable of taking steps to protect himself from fraud and financial harm. That is to say there was more he might reasonably have done that would have led to the scam being uncovered.

Mr J was actively looking for investment opportunities and he was not under any threat or pressure to make the payments. The payments were spread out over a period of time and there would've been enough time and opportunity to make further enquiries before proceeding. I believe his actions after he made the payments when he challenged the next KYC (know your customer) fee show he was capable of considering complex issues and seeking answers.

Having thought very carefully about everything Mr J's representatives has told us, whilst I'm not saying Mr J's circumstances had no impact on him at the time, I'm not persuaded that it would be unreasonable to expect him to have protected himself against the particular scam he fell victim to. And so, I don't find that Lloyds need refund Mr J's entire loss under the vulnerability clause of the code.

Did Lloyds do enough to recover Mr J's funds?

I've also thought about whether Lloyds took reasonable steps to recover Mr J's funds once it was made aware he was the victim of a scam. The first scam payment was made on 3 November 2021 and the last one on 22 November 2021. Mr J reported the scam on 13 December 2021. Lloyds contacted the beneficiary bank on the same day a few hours later but no funds remained. I've seen the evidence to show funds were removed shortly after (within minutes or hours of) being deposited on each occasion. So, even if Lloyds could have contacted the beneficiary bank immediately after Mr J reported it, I don't consider it would make a difference in this case as the funds were removed within hours of being transferred - well before Mr J reported the matter to Lloyds.

My final decision

For the reasons above, my final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr J to accept or reject my decision before 28 September 2023.

Kathryn Milne
Ombudsman