

The complaint

A company which I will refer to as 'R' complains that Lloyds Bank Plc failed to prevent a scam which R fell victim to, and then refused to reimburse the loss they incurred as a result.

For avoidance of doubt, this complaint is solely about Lloyds as the recipient's bank.

What happened

The background to the complaint is known to both parties and so I won't repeat it at length here.

Briefly, in January 2022, a scammer intercepted an existing email thread between R and its supplier and provided R with an invoice with amended bank details. Before making the payment, which was about £53,000, R noticed the change in the bank details and attempted to call the supplier twice to confirm the change, but they did not answer.

The next day the scammer emailed pursuing R for payment. R replied (without realising that it was the scammer) asking them to confirm the new bank details, which they did. R proceeded to set up the payment using the account details provided on the invoice. During the payment process R was presented with a 'no match' Confirmation of Payee (CoP) message. R tried to make the payment again and again received a 'no match' warning. R then emailed the 'supplier' asking for confirmation of the recipient's account name. The scammer responded by providing a completely different name. This time the payment went through.

The scam came to light two days later when R's supplier advised R of non-payment. R reported it to their bank (part of Lloyds Banking group) who in turn commenced an investigation. Unfortunately, by that time only about £130 remained in the recipient's account. Lloyds however were able to retrieve a further sum of about £17,000 from third party accounts. So, the net loss to R is about £37,000. Lloyds did not agree that it was at fault. It said that the bank completed full due diligence when the recipient's account was opened and did not have any concerns. In addition, the bank had no concern about the account activity. It also said that it acted swiftly upon being advised of the scam and managed to recover about £17,000.

One of our investigators considered the complaint and concluded that it should be upheld. They said, in summary:

- Lloyds did not provide a copy of the account opening documents, so it cannot be said with certainty that it opened the account appropriately or met its regulatory obligations.
- In any case, the incoming payment from R and the payments that swiftly went out of the account were unusual to the normal account activity and as such ought to have prompted Lloyds to look into what was going on. Had the bank done so and questioned its customer about the nature of the transactions, the scam would most likely have come

to light and that in turn would have prevented the financial loss to R. So, it is fair that Lloyds refunds the loss.

- However, there was some contributory negligence on part of R. They did try to call their supplier to confirm the change in bank details and were not able to contact them on the first day. But when the scammer chased them for payment, they sought confirmation of the change of account details via email only. Further, when they initially set up the payment, a CoP mismatch message was presented twice. When they queried this via email, the scammer gave an altogether different name. That name indicated a line of business ('cleaning services') which was too remote to the supplier's line of business which was a manufacturer of industrial equipments (and whom R said had been their supplier for many years).

All of this taken together ought to have prompted steps to have been taken to speak to the genuine supplier again on the phone before making the payment. Had R done so the scam would have come to light.

So, the investigator concluded that the liability should be shared equally between both parties, and it is fair that Lloyds reimbursed 50% of the loss R suffered, with interest.

R accepted the investigator's opinion, but Lloyds didn't. The bank said, in summary:

- The investigator's comments that alerts should have been flagged when the funds credited the account and quickly removed are with the benefit of hindsight looking back at earlier transactional history. The anti-money laundering transaction monitoring landscape is inherently a post-event control seeking to identify unusual behaviour aligned to AML typologies. As it is a post-event control, the bank does not believe it is applicable for the circumstances of this case.
- The account in question was correctly opened with full KYC checks completed in line with legal and regulatory requirements, and normal procedures.
- In addition, the bank had no concerns with the account and there was no fraud trigger in respect of the subsequent outbound payment activities. Therefore, the bank had not acted unfairly or unreasonably in the circumstances. Even if the bank had stopped the outgoing payments and contacted its customer, it would have been easy for them to satisfy any concerns as the payments were authorised by them.

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.

Lloyds has an ongoing obligation to be alert to various risks in relation to accounts with it. Specifically, I'm mindful that it:

- must conduct their business with due skill, care and diligence;
- has a longstanding regulatory duty *"to take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be*

used to further financial crime” (SYSC 3.2.6R of the Financial Conduct Authority Handbook);

- must fairly and reasonably been monitoring accounts and any payments made or received to counter various risks including anti-money laundering and preventing fraud and scams. At the material time, those requirements included maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage risk, e.g. through customer due-diligence measures and the ongoing monitoring of the business relationship including through the scrutiny of transactions undertaken throughout the course of the relationship;

I am also mindful of what the Payment Systems Regulator has said about the role of receiving PSPs in relation to authorised push payment fraud. For example, in the “Which? authorised push payments super-complaint PSR response December 2016”, they have said:

“APP scams can be prevented by receiving PSPs monitoring inbound payments and intervening where they identify suspect transactions”

“We consider that receiving PSPs may potentially be able to do more in terms of proactively monitoring inbound payment activity to help prevent APP scams. ..”

“In terms of regulatory obligations, those PSPs that come under the FCA’s Handbook, such as banks and building societies, are obliged to have adequate policies and procedures to counter the risk that they might be used for financial crime, including fraud.”

“Since PSPs face ongoing duties to prevent financial crime (SYSC 6.3.1 and SYSC 6.3.3), the need to conduct customer due diligence checks does not end once the account is open. An account that passed all the appropriate checks when it was opened may be used for fraudulent purposes at a later date.”

Likewise, a bank must have systems in place to look out for unusual transactions or other signs on its customer’s account that might indicate risk of fraud. This is at the very least to ensure that their own customer hasn’t fallen victim to a scam, particularly given the increase in sophisticated fraud and scams in recent years.

Ultimately, it is a matter for the bank as to how it chooses to configure its fraud detection systems and strike a balance between allowing its customers to transact business and questioning transactions to confirm they are legitimate. But where a complainant alleges that that a bank didn’t do enough to prevent a loss which resulted from an APP fraud, I will look into the circumstances of the case and decide based on what I have seen, whether, in that case, the bank could have fairly and reasonably done more.

The bank has provided relevant information to our service to allow us to investigate this. I am limited as to how much information I can share because it relates to a third-party account. But I’d like to assure R that I’ve carefully reviewed everything before reaching my decision.

Having reviewed the submissions, I agree with the investigator that Lloyds could have done more here to help prevent the loss to R.

Account opening

We have not been provided with a copy of the account opening documents by Lloyds despite requests. So, it is difficult for me to safely conclude that there was nothing of concern at the account opening stage.

Nevertheless, it is my view that Lloyds in any case missed a subsequent opportunity to prevent the financial loss to R.

Account activity

Briefly, as I understand it, the recipient's account was opened about a year prior to R's money arriving in the account. During this period, I can see that there was hardly any activity on the account. There were just one or two very small payments in and out.

It was in these circumstances R's payment of nearly £53,000 came into the account. This was an unusual transaction compared to prior account activity, and also of very high value. This was then followed by a series of large payments out of the account. Lloyds has not provided us with the times when these payments went out. However, from the bank statement it appears that the first outgoing payment was for £8,000. This outgoing payment was also unusual to the previous account activity and far greater than the only payment of £130 made out of the account during the entire year prior to this. This was then followed by a series of large payments on the same day. In fact, the whole of R's £53,000 was transferred out via multiple payments on the same day.

Given all this, I agree with the investigator that there was enough going on here that ought to have prompted Lloyds to take a closer look at what was happening, at least when the first payment was made out of the account, if not earlier.

The bank says that the investigator's opinion that alerts should have been flagged is with the benefit of hindsight looking back at earlier transactional history. However, I consider that previous account activity is a key factor for a bank to decide - at any given point in time - whether or not an alert ought to be flagged. So, I don't accept that looking at the earlier transactional history to decide whether an alert ought to have been flagged is with the benefit of hindsight.

I cannot be certain as to what would have happened had the bank intervened. So, I will have to consider what more likely would have happened had the bank contacted its customer and if they were reachable.

It may be, to start with, the bank's objective would have been to look out for unusual transactions going out of the account in order to protect its customer from the possibility of fraud. But that would have given the bank an opportunity to look more closely at what was going on. Had it done so, it would have noticed that after very little activity for more than a year, an unusually large amount was received.

The bank says that even if it carried out further investigation, their customer would have been able to satisfy any concerns about the incoming payment. Further, even though their customer's stated business was 'cleaning', it was entirely possible that R could have had a 'business need for cleaning services'.

However, the bank would have been able to see from its records that their customer's business supposedly started a year ago. So, by the time these transactions happened a year later, it would be reasonable to expect some business related transactions on the account, as for example purchase of materials and payment of wages. But there was hardly any activity on the account. Thus, their customer received a large sum of £53,000 without any evidence of prior business activity.

If the customer claimed the £53,000 – which was a large sum - as a payment for cleaning services already carried out by them, then it is reasonable to expect that, beforehand, there

was sufficient activity on the bank account such as payment to staff and other overheads. But there were no payments at all such as for materials, salary, direct debits, utility payments and everyday expenses which one could reasonably expect to see in a business account.

If the customer were to present this as some advance payment, then there ought to be some correspondence between R and them to evidence this. But it is more likely they wouldn't have been able to show any email exchange or correspondence between their business and R justifying these payments, as none such existed.

I have taken into account what the bank has said, and I acknowledge that it is difficult to know for certain what would have happened had the bank intervened early on and questioned its customer about the source of incoming payments. But taking all of the above into account, I am not persuaded, on balance, that their customer would have been able to provide a credible explanation given the anomalies.

Generally, when there are concerns about a payment (or payments), banks do tend to thoroughly investigate the matter. And had Lloyds done so, I think it would have, during this time received the scam notification from the remitting bank.

Thus, I think the bank missed an opportunity here to help prevent the financial loss to R. Therefore, it is only fair that it compensates R for losses that it would not have suffered but for the bank's failures.

Did R act reasonably in the circumstances?

For completeness, I've also considered whether R should bear some responsibility for their loss due to any contributory negligence. Having done so, I agree with the investigator that R could have done more to prevent the scam for the reasons given by them. However, this does not negate the fact that Lloyds too missed an opportunity to prevent R's loss, as described above.

In the circumstances I consider it fair that the loss is shared equally between Lloyds and R.

Putting things right

As I understand it, the total payment made to the fraudster was £52,800. Of this, £16,953.31 has since been recovered leaving a loss of £35,846.69. I ask R to confirm that they had not received any further payments from any other source such as their insurers.

For the reasons given, this loss should be borne equally by Lloyds and R. This means Lloyds should reimburse £17,924 to R. It should also pay interest on this sum.

The funds were lost from a business current account, which earned little interest. But the relevant question is the opportunity cost of the lost funds to R. In this case, I cannot be certain about the cost to R of being deprived of the money because it might have used the funds in a variety of ways. It is however clear to see that this was a large sum of money, and the loss has had a big impact on the company. In the circumstances, without any compelling reason to depart from our usual approach, I consider it fair and reasonable that Lloyds pay R simple interest at 8% p.a. on the sum reimbursed.

The investigator has said that the interest should be paid from the date when R made the payment to the genuine supplier (which I understand was about three weeks after the fraudulent transaction) to the date of settlement. I accept it is a reasonable time period.

My final decision

My final decision is that I uphold the complaint.

In full and final settlement of it, Lloyds Bank Plc should pay R 50% of the loss it incurred together with simple interest at 8% p.a. Interest should be paid from the date R paid its supplier to the date of settlement.

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

Raj Varadarajan
Ombudsman