

The complaint

T complains that London Community Credit Union Limited (LCCU) didn't do enough to prevent the loss caused to them as a result of an authorised push payment ('APP') fraud.

What happened

The background to the complaint is known to both parties and so I won't repeat it at length here. Briefly, in early June 2019, T fell victim to an invoice interception scam which resulted in them making two payments totalling about £26,000 to an account with LCCU. The fraud came to light a week later when the genuine supplier contacted T after non-receipt of the payments. T contacted its bank who in turn contacted LCCU, but it appears that no money was left by then on the recipient's account.

T complained to LCCU that it failed to prevent the fraud. They asked what checks were done by LCCU prior to accepting the membership of its customer, and why it failed to act when large payments came into the account and was withdrawn so quickly. LCCU said that it hadn't made any mistake.

Our investigator concluded that LCCU could have done more to prevent the loss to T. They said it isn't clear from the information provided by LCCU whether, when their member's account was opened, LCCU could have reasonably foreseen that the account would be used to receive fraudulent credits. They said that in any case, the relevant incoming transactions and the related outgoing payments were unusual activities to the recipient's account. So, the investigator was of the view that had LCCU held the first large payment going out of the account and looked into things, it would have had an opportunity to prevent the fraud from occurring. But it failed to do so and therefore it is fair that it compensates T for the loss arising from the fraud.

LCCU didn't agree. It said, in summary:

- T did not perform the checks that could reasonably be expected of them when dealing with what appeared to be a change of account details of a supplier.
- Tight procedures were in place when the recipient account was opened and valid evidence obtained. LCCU had no concern at the time the recipient account was opened.
- LCCU met its obligations in carrying out the transactional monitoring as it investigated the source of funds with the sender bank.

On further querying the final point, LCCU told us that the first incoming payment was flagged due to certain triggers. Following this it called the sending bank who said that they had not raised any suspicion over this payment and nor their customer. And on this confirmation the suspension was lifted. When the second incoming payment arrived, there was a trigger again but as LCCU had already cross checked the initial funds with the sending bank it felt that there was no need to repeat the process with the second payment.

LCCU provided a screenshot of its system evidencing that it called the sending bank, but it wasn't able to provide any call recording. It said that this is because the call happened more than two years ago.

Following this, our investigator contacted the sending bank who said that there is no record of a call from LCCU on T's file. They said that their process is to make a note on the account if such a contact was received and there is no such note in their records. They provided us with T's account notes as evidence of this. They further said that they also searched their general call database for calls from LCCU from its main number (which later LCCU has confirmed is the correct number), and in all of June 2019 there were only four calls from LCCU but none of those related to T.

Following this, our investigator wrote to LCCU that on balance they can't be certain whether LCCU reached out to the sending bank. The investigator said that in any case they can't see that LCCU contacted their own customer or that they looked into the fact that the name on the payment didn't match their customer's account once it was flagged. So, they remained of the view that LCCU missed an opportunity here to help prevent the fraud, resulting in a financial loss to T.

LCCU responded to say that it would contest any suggestion that it did not call the sending bank. It reiterated that it did enquire with the sending bank and their notes suggest that these enquiries satisfied any suspicion LCCU had. It also reiterated that T failed to check with the genuine supplier the bank details before making the payment.

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.

Having done so, I agree with the investigator's conclusions essentially for the same reasons.

In broad terms, the starting position in law is that a financial business like LCCU is expected to process payments and withdrawals that a customer (its member) authorises it to make, in accordance with the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case. But that is not the end of the story. LCCU also 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*" (FCA Principle for Businesses 2);
- have 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, which has applied since 2001);
- must fairly and reasonably be 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;

- must have systems in place to look out for unusual transactions or other signs that might indicate risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years.

Ultimately, it's a matter for LCCU 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 it is alleged that it 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 LCCU could have fairly and reasonably done more.

Taking all of this into consideration, I think in this instance LCCU had reason to have done more. I will explain why.

LCCU hasn't provided us with the account history of their customer despite our requests. However, I note that LCCU doesn't dispute that the incoming and outgoing payments were unusually large for the account. Also, it hasn't provided us with any evidence to show that payments of this nature were in line with the regular or expected activity on this account.

In fact LCCU says that the first incoming payment was flagged due to certain triggers, in particular the size. It says at that time it contacted the sending bank who confirmed that they do not have any suspicion over this payment and nor their customer. The sending bank on the other hand is adamant that it did not receive any call from LCCU about this. And as I previously noted they have provided us the historical account notes of T. This doesn't show that there was a call from LCCU concerning T's account as claimed by LCCU.

If there is a dispute about what had happened, I must decide on the balance of probabilities – in other words, what is most likely – in the light of the evidence.

LCCU isn't able to produce the relevant call recording with the sending bank. It says that this is because the call took place two years ago. However, I note that we asked for its case file within a few months of the event happening.

Even if I accept that LCCU called the sending bank, I can't know with certainty what exactly it asked the sending bank. For example, did LCCU discuss the implication of the mismatch in the payee name – which is something I would expect LCCU to ask the sending bank if the purpose of the call was to verify the genuineness of the payment.

LCCU says that it asked a series of questions requiring 'yes' or 'no' answers and one of the questions was: 'Confirm the Sender and Receiver Account details'. If such a question was asked, I think it is likely that the mismatch of payee names would have come to light. In such circumstances it seems unusual to me that the sending bank would confirm there and then that it had no suspicion about a payment without checking with its customer. And if it did check with its customer, I consider it more likely that it was recorded in the account notes or T would have had a recollection of it.

I have carefully considered what LCCU has said but in the absence of corroborating evidence and for the reasons I have explained, I cannot be certain whether LCCU reached out to the sending bank and even if it did, whether it asked the questions relevant to this case in order to verify the genuineness of the payment.

In any case, I think that there was enough going on here in terms of incoming and outgoing payments that ought to have raised concerns to LCCU prompting it contact its customer about the transactions. There is no evidence that it did. The information the police has provided to T indicates that the recipient had admitted to having their account used as a

'money mule', that they didn't send any of the fraudulent emails or transferred the money onwards electronically but a third party was responsible for all these. Given this, I think that had LCCU contacted its customer and asked the appropriate questions including about the mismatch in payee's name, it is more likely that their customer wouldn't have responded plausibly or at all. This would have prompted further investigation and allowed time for the notification to be received by the sending bank, ultimately preventing these funds being fraudulently used.

For completeness, I've considered whether T should bear some responsibility for their loss due to any contributory negligence. But in the circumstances of this complaint, I don't think they should. T was going about its business in the usual way without knowledge or awareness of the fraud. When they received the intercepted email, the email address appeared very similar to their actual supplier's address and the request itself wasn't out of the ordinary. They were expecting the invoice from their supplier. Further, I can see that they took steps to verify that the request was genuine and asked for a signed document from the supplier confirming the change in account details. And they did receive a document purportedly signed by the executive director of the supplier. Unfortunately, the document provided was also fraudulent, but T wasn't aware of all this at the time. So, in the circumstances I can't fairly conclude that they acted unreasonably.

I appreciate that LCCU needs to strike a balance in the extent to which it intervenes in payments, against the risk of unduly inconveniencing or delaying legitimate payment requests. I also acknowledge the main perpetrator here is the fraudster.

However, for the reasons explained, LCCU could have done more to help prevent the loss to T, but it failed to do so. Therefore, it is fair that it refunds the sum lost by T as a result. I also consider that 8% simple interest should be added to compensate for T being without funds they otherwise would have had. Interest should be paid from the date T (or its bank) first raised the fraud claim with LCCU until the date of settlement.

My final decision

My final decision is that I uphold the complaint. In full and final settlement of the complaint, LCCU should pay £26,533.93 to T together with interest as I have set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask T to accept or reject my decision before 11 March 2022.

Raj Varadarajan
Ombudsman