DRN-4638450

The complaint

A company which I'll call 'B' complains that Lloyds Bank Plc didn't reimburse the money it transferred to a fraudster.

The complaint is brought on B's behalf by one of its directors, Mr A.

What happened

Both parties are aware of the circumstances of the complaint, so I won't repeat them all here. But briefly, B received an invoice from what it believed was an existing supplier's email address requesting a payment of £54,666.41. B says it was expecting the invoice from the genuine supplier and had been in contact with them with regards to some outstanding payments. B also says that the email address was virtually identical, and the content and language used didn't raise any suspicions.

The company says that it made a £1.00 payment to check the account details were correct and after checking this payment had been received, it made a payment for the outstanding balance of £54,665.41. Once the genuine supplier contacted B around a week later to chase the invoice payment, the scam was discovered, and Mr A immediately called Lloyds, followed by the police.

Lloyds is a signatory of the Lending Standards Board's Contingent Reimbursement Model Code ('CRM Code') which requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances.

Lloyds looked into the matter but didn't refund B. It said that one or more of the exceptions to the CRM Code applied in this case, specifically it says that B didn't have a reasonable basis for belief when paying the invoice and that it had provided effective warnings to B. Lloyds did contact the receiving bank to see if it could recover any of the money paid, but it was only able to recover £16.83 which was returned to B. Lloyds also didn't think it had done anything wrong in its escalations to the receiving bank to attempt recovery of the funds.

Our investigator recommended the complaint be upheld. He thought that Lloyds should refund B the whole of their loss, less the £16.83 recovered from the receiving bank, along with 8% interest. He thought that B had a reasonable basis for belief as it was expecting an invoice from this supplier and the email address used by the fraudster was almost identical to that of the genuine supplier. He also thought that B had tried to take precautions by making an initial small payment, and had a reasonable explanation for why it thought it had received a 'Confirmation of Payee' ('COP') no match when making the payment.

Lloyds didn't agree. It said in summary that:

- When Mr A had made the complaint to the bank, he said that B hadn't followed its own internal procedure, which was to call the supplier if they were new or had changed account details.

- B was in regular contact with the genuine supplier but didn't discuss the change in

account details with them.

- Even though B followed its internal process and sent a payment for £1, if it didn't call the supplier on an existing number then this process was irrelevant.

- B received a relevant warning before making the payment saying that scammers could hack emails and to check with the payee to see if their payment details had changed – but not to use the contact information contained in email and/or invoice.

- B had received a COP 'no match' when making the payment.

As an agreement couldn't be reached, the case has been passed to me to decide.

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 am satisfied that under the terms of the CRM Code, Lloyds should have refunded the money B lost.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to consider relevant: law and regulations; regulators' rules, guidance, and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

The starting point for my considerations is that, under the Payment Services Regulations 2017 and the terms of its account, B is liable for transactions it has carried out itself. However, Lloyds has agreed to consider claims in line with the CRM Code and also has legal and regulatory obligations to be on the lookout for unusual and out of character transactions which might indicate that its customer is at risk of financial harm from fraud.

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. I have set out the relevant exceptions which Lloyds believes apply to this case below:

- The customer did not take appropriate actions following a clear negative Confirmation of Payee result.

- The customer ignored what the CRM Code refers to as an "Effective Warning" by failing to take appropriate action in response to such an effective warning when: setting up a new payee, when amending an existing payee: and/or immediately before making the payment.

- The customer made 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.

- Where the customer is a micro-enterprise or charity, it did not follow its own internal procedures for approval of payments, and those procedures would have been effective in preventing the APP scam.

There are other exceptions, but they don't apply in this case.

I've carefully considered Lloyds' representations about the warnings it gave and whether B had a reasonable basis for believing the transaction to be genuine. But they don't persuade me to reach a different view to that of our investigator. In particular I am not persuaded that Lloyds has been able to demonstrate that any of the exceptions to reimbursement apply.

Confirmation of Payee (COP) – Did Lloyds meet its obligations under the Code and did B ignore a clear negative confirmation of payee warning?

The CRM Code says that where a Firm identifies an APP scam risk in a payment journey, such as where an existing payee's details have been amended, they should take reasonable steps to provide their customers with effective warnings. These warnings should include appropriate actions that the customer can take to protect themselves from APP scams. Here, B was paying an invoice to an existing supplier for £54,666.41, but using new account details. So, when B decided to make a payment via internet banking to these amended details, this would likely have been identified as a potential scam risk.

Lloyds told us that B was presented with several messages throughout the payment journey that should have alerted it that something was wrong. The first of which was a COP 'no match' alert which said:

> "*Recipient name and account details don't match*
>
> *This may be because:*
>
> - *You entered a profession or service instead of a name*
> - *You entered a person's name instead of a business name*
> - *It's the wrong account number*
>
> ***Check before you pay***
> *Confirm the account number, sort code and name with the recipient. Call them on a number you trust, not one from an email or invoice.*
>
> ***Stay safe from scams***
> *Fraudsters can email new account details as part of a scam. If you pay details that don't match and it's a scam, it's very hard to get the money back."*

The second of which said:

> "*Recipient name and account details still don't match*
>
> *You should check the following details with the recipient:*
>
> - *sort code*
> - *account number*
> - *name on the account*
>
> *Call them on a number you trust, not one from an email or invoice.*
>
> ***Stay safe from scams***
> *Fraudsters can email new account details as part of a scam. If you pay details that don't match and it's a scam, it's very hard to get the money back."*

So, I'm satisfied that Lloyds identified there was a risk to B of an APP scam, but I'm not persuaded by the bank's argument that these messages should have raised more concerns for B than it did. Whilst I acknowledge that the COP no match message appeared to catch Mr A's attention, I'm satisfied that the company did what it thought was required to check the account information was correct when it sent the £1.00 payment (Mr A says that he doesn't remember receiving any messages and/or warnings on his internet banking for the second payment of £54,665.41).

Furthermore, Mr A told us that B's supplier had previously operated under a different name, so it didn't seem odd that the name on the account might not match or that it had received a COP 'no match' warning when sending the payment to the supplier. And he held the same belief when the second warning was presented which said the details *still* didn't match, as Mr A remained of the opinion that this meant the account name was in the supplier's original name.

I think it's also worth noting here that B told us it had been undertaking a wider reconciliation exercise with the supplier for some outstanding payments and had been in regular contact with the supplier over a lengthy period. So, receiving this 'fake' invoice in the way it did didn't seem unusual as it had already been reviewing numerous payments as part of a wider exercise in reviewing outstanding/missing payments, so it didn't appear out of the ordinary. And given that B was reviewing these missing payments with the supplier, I don't think the change in bank details would have appeared odd under these circumstances – particularly as B is a small firm without extensive knowledge of intercept scams. I'm also satisfied that B didn't understand the financial consequences for the company of the COP 'no match' warning, given the irrevocable nature of the 'faster payments' it had used to make the payments, and what would happen in the event the funds were received by a fraudster.

Effective warning – Did Lloyds meet its obligations under the Code and did B ignore an effective warning?

The CRM Code says that where an "effective warning" is provided, it should be risk based and, where possible, tailored to the APP scam type. It must also provide information that gives customers a better chance of protecting themselves against fraud or scams, like that experienced by B in this case. When reviewing any warning given, consideration must also be given to whether the warning is likely to have had a material impact on preventing the scam. The CRM Code therefore sets out minimum criteria which must be met for a warning to be effective. The criteria says that a warning must be understandable, clear, timely, impactful, and specific.

Lloyds told us that the COP no match was only one of the warnings that B was given when attempting to make the initial £1.00 payment and should be considered in conjunction with the addition warning B was also given which said:

> *"**Don't pay until you check***
>
> *Fraudsters sometimes hack into suppliers' email accounts and send out fake invoices or new bank account details.*
>
> *If you get an invoice by email, call the supplier to check the details before you make this payment. Use a phone number you have stored for them – not one listed in the email."*

Lloyds told us that it believed its warnings were effective and therefore the relevant exception could be applied. However, I'm not satisfied this warning meets the definition of an 'effective warning' as set out in the CRM Code. I say this because, although the warning

attempts to touch on this type of intercept scam, I'm not persuaded it gives enough information to bring to life what an invoice intercept scam (like the one B has fallen victim to) would look or feel like, nor does it highlight the common/key features of this type of scam which would resonate with B.

The warning itself also doesn't explain that fraudsters often build rapport with those they are targeting to gain their confidence before changing details or sending fake invoices, and that once the payment is made, it is not reversable. So, I don't think the warning itself was impactful and would have alerted Mr A to the type of fraud B experienced here. Furthermore, Mr A told us that he only remembered receiving a warning for the £1.00 payment not the second payment for £54,665.41, and given that there was about twenty-four hours between the first and second payments being made, I'm also not persuaded that Lloyds warning here was timely either.

Did B have a reasonable basis for belief?

Lloyds also says that its decision not to refund B under the CRM Code was justified, as the company didn't have a reasonable basis for believing that the payment it made was genuine. But I don't agree. I've looked at the correspondence received from the fraudster and the genuine supplier, and the content, tone and language were similar from both parties. I don't think there was anything within the emails to cause B to think it was speaking to anyone that wasn't the genuine supplier – particularly as the fraudster referred to other members of staff and transactions that hadn't been referred to throughout the previous email correspondence or the fraudulent invoice.

Looking at the wider circumstances here, B had been regularly engaging with the genuine supplier regarding outstanding payments. This meant that B was expecting an invoice from the supplier, so they had no reason to question the timing and nature of the invoice request – particularly as the total invoice was a consolidation of smaller payments which B had been reviewing with the genuine supplier.

Furthermore, I've seen that the sending email address itself from the fraudster is very similar to the genuine supplier, and I think it's reasonable that B did not identify that one digit was different in the email address when considering the wider context of the email itself. I'm not persuaded there was anything unusual that would have raised B's suspicions here that something was wrong with the request it received. So, I think B did have reasonable basis for believing that the payment it was making was genuine and I'm not persuaded by Lloyds' argument that a CRM Code exception should apply here.

Did B follow its own internal process?

Lloyds told us that B didn't follow its own process when making this payment. It says B told the bank, when reporting the suspected fraud, that its process was to make a call before paying an invoice to a company it hasn't paid before, or where any bank details have changed. However, that didn't happen for this payment and therefore the relevant CRM Code exclusion should apply.

B told us it does have a process in place to call for certain invoices, but this is only for 'new suppliers' where it hasn't previously made a payment. Therefore, as this was an existing supplier, they didn't actually have a 'formal' process in place. I've listened to the calls with B and Lloyds, and I'm not persuaded by the bank's view here that B said it should have called the supplier to confirm the details and therefore that was B's process and B's own actions led to the loss.

I recognise that Lloyds disagree with me about the context of the words used by Mr A when speaking to the bank. However, I remain of the opinion that the comments used appears to have been made to describe what would have been the ideal solution to prevent the situation using the benefit of hindsight, i.e., confirming the account details using email rather than phone 'that was her mistake' and 'she should have called to confirm the details with the supplier rather than sending an email' and not because this was the company's actual process. B even confirmed this in the follow up call with Lloyds when questioned about making calls as part of its process. It said, "*it is our process now*." So, I'm not persuaded that B didn't follow its own process at the time in question.

B told us that it did have some concerns after receiving the COP 'no match' warning, so despite thinking this may be due to the change of business name, it took an additional precaution by making a smaller interim payment. B told us that it made a small £1 payment as it wanted to check the new details were correct, and that its accounts person then followed this up to confirm the £1 had been received. Then, once this had been confirmed, the remaining balance was transferred.

I recognise that Lloyds says B should have called the genuine supplier based on the warnings it received. However, as B has explained, it doesn't have a process in place for payments of this nature and I think the evidence shows that B believed an email would be sufficient instead. It is unfortunate that B replied through the same email chain with the fraudster who had sent the amended bank details. However, given B's relationship with the genuine supplier and the ongoing correspondence regarding the reconciliation, I think B's actions were reasonable.

Should Lloyds have done more to protect B?

I've thought about whether this payment was unusual and out of character. B's account statements show the largest single payment from its account was for around £31,500 – and this was unusual. Generally, the largest payments from B's account were around £15,000 and were paid by direct debit, so the fraudulent payment was much larger and out of character for B's account. I think it's also worth noting here that Lloyds itself observed that B did often make payments in a similar way, but these were much smaller, and that the only other payments of a larger size were to HMRC.

So, based on what I've seen, I think Lloyds should have done more here than just displaying warnings, by contacting B and questioning the payment at the time it was making it. If Lloyds had done so, I think it's more likely than not that the bank would have asked more questions about the payment, which with its knowledge and experience with this type of fraud, would likely have brought the scam to light. The relevance of this, is that I think Lloyds could have done more here to prevent the scam and therefore I think the bank should pay B interest on the redress from the date of loss, instead of the date it decided not to refund B under the CRM Code.

Recovery of funds

The CRM Code says that where an APP scam is reported to a firm, the sending firm should:

- Notify any UK receiving firms in accordance with the procedure and timeframes set out in the Best Practice Standards

- If a firm is not a signatory to the Best Practice Standards, the Firm must have in place equivalent procedures to notify UK receiving Firms in a timely manner

Lloyds has provided us with evidence which shows that Mr A contacted it at around 14:40 on 22 November 2022, and it subsequently logged a fraud complaint and contacted the beneficiary bank (who had received the funds) at 15:30 on the same day. I've also seen evidence that Lloyds was regularly chasing the beneficiary bank to see if any of B's funds remained so that these could be returned to the business. So, I'm satisfied that Lloyds met its obligations here in line with the best practice standards in its attempts to recover B's funds from the scammer's account.

Overall

I have carefully considered Lloyds' arguments about the warnings it gave and whether B had a reasonable basis for believing the payment to be genuine. But overall, I'm not persuaded that Lloyds has demonstrated that it may rely on any of the exceptions to reimbursement in the CRM Code. So, I think it's fair that Lloyds now refunds the money B lost as a result of the scam along with interest.

My final decision

My final decision is that I uphold this complaint. I instruct Lloyds Bank Plc to do the following:

- Refund B the money that was lost in the fraud, less the £16.83 which was recovered.
- Pay 8% simple interest from the date the payment was made until the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask B to accept or reject my decision before 22 October 2024.

Jenny Lomax
Ombudsman