DRN-3747151

The complaint

Mr H, as a director of S (a limited company), complains that Starling Bank Limited (Starling) won't refund S for a loss they suffered as the result of a scam.

What happened

The background to this case is not in dispute so I won't be going into details. In summary, an employee of S was completing a university course while working for them. S was due to pay for the next year's study costs for the employee and received an invoice from the university. This email was intercepted by a fraudster who changed the bank details and received the money, rather than the university S expected to pay.

S made two separate payments to the fraudster. On 29 March 2021 they paid £1,000 and on 30 March 2021 they paid a further £3,500.

S says they received a Confirmation of Payee (COP) no match, so they contacted the university to check the payment details. But, due to Covid, the accounts team were working off site and weren't taking phone calls. S says they were told to check the invoice details for the bank information, so proceeded with making the payment.

S became aware they'd been the victim of a scam when the university got in touch later, asking for payment of the course fees. S contacted Starling immediately and raised a fraud claim, asking Starling to reimburse them.

Starling considered S's claim in line with the Lending Standards Board's Contingent Reimbursement Code (the CRM Code), but declined to refund S saying:

- S ignored warnings provided by Starling at the time of making the payments.
- S didn't do enough checks prior to making the payment and should've taken further precautions to find out why the beneficiary account information had changed.

S wasn't happy with Starling's response, so they brought a complaint to our service.

An investigator looked into S's complaint and upheld it. They explained to Starling that the warnings provided to S didn't meet the definition of an "Effective Warning" under the CRM Code, and therefore Starling couldn't rely on them as a reason not to refund S. The investigator also felt that S made sufficient checks and had a reasonable basis to believe they were paying the university - therefore Starling couldn't rely on that as a reason not to reimburse S either. The investigator recommended that Starling reimburse S in full and awarded interest at 8% simple.

Starling disagreed with the investigator's opinion, giving the following reasons:

- One of the emails from the fraudster showed that their email address was different to the genuine sender S had been dealing with. Also, the signature under the sender's name had changed.

- S should've been concerned that they were being asked to pay an individual trading as the university.
- S's first payment was restricted to only £1,000 due to a Confirmation of Payee (COP) no match – meaning that the payee information on the payment couldn't be matched to the account holder name. Therefore, S should've done more checks
- S selected the wrong payment purpose when making the payment, which meant they weren't shown the correct warning. If they'd correctly selected "invoice/bill" rather than "purchase" the warning they would've seen would've made more sense.
- The university's correct payment information was available on their website and Starling believe if S had called the university it's likely they would've directed him to their website – which would've highlighted that the bank details didn't match.

As Starling disagreed with the investigator's opinion, the case was passed to me to review.

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.

Starling are a signatory of the Lending Standards Board's Contingent Reimbursement Model (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. Starling says two of those exceptions apply in this case.

Under the CRM Code, a bank may choose not to reimburse a customer if it can establish that*:

- 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
- 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.

* there are further exceptions outlined in the CRM Code, but they don't apply to this case.

Did Starling provide an effective warning as defined by the CRM Code?

When S set up the new payee to pay the university, Starling say they would've seen the following warning, "could this payee be part of a scam? Always verify who you are sending money to as you may not be able to recover these funds…"

Starling also say S was provided with a warning based on the payment purpose they chose of "purchase". That warning said "Fraudsters often pretend to sell items online. They'll take your money and send you nothing in return. If you have not seen the item in person perform checks on the seller….".

Having considered both warnings, I'm not satisfied that they meet the definition of effective warnings as set out in the CRM Code – for the following reasons:

- The new payee warning doesn't include any information about the type of scam S may've fallen victim to, what steps S should take to protect themselves, and requires

S to click through a link to Starling's website to find out more information about scams. I'm not satisfied that this would've been impactful as S was expecting to receive the invoice from the university and the amount requested matched the information they'd been given about the payment. So, I'm not satisfied that this warning would've been impactful to S.

- The payment purpose warning relates to buying something online and is more relevant to someone who may've made a purchase on an online marketplace. The warnings isn't relevant to the scam that S was the victim of. They had been dealing with the university for some time and the payments there were asked to make matched the fee they'd been quoted in earlier emails. Also, the suggested steps set out in the warning, wouldn't have helped S avoid falling victim to this scam.

Starling have referred to the warning S would've seen had they selected a different payment purpose of "invoice/bill".

The invoice/bill warning says, "Fraudsters can take over email addresses or call from seemingly reputable numbers, posing as genuine organisations or business associates. Have you been asked to make an unexpected payment? Have you been told that the account details for a payment have been changed? Check any unexpected or amended instructions via a trusted channel that is separate to the one that they used to contact you. Visit the website to learn more about how to protect yourself from fraud".

However, I'm not satisfied that even if S was presented with that warning it would change the outcome, as I'm not satisfied that it was an effective warning, or that S ignored it.

- In this case, S hadn't been asked to make an unexpected payment so that didn't apply to their scam.
- The instructions in the email weren't unexpected or amended as referred to in the warning. The email continued on a chain with the genuine university contact, the amount they were asked to pay was the expected amount previously discussed, and all of the information provided in the email matched what S expected.
- Also, S had contacted the university by phone, as suggested by the warning. However they were only able to proceed based on what the university told them which was to use the information that had been provided on the invoice. S were specifically told that they couldn't talk to anyone in the accounts team. So, S took the recommended steps suggested in the warning and didn't ignore them. Also, I'm conscious that this warning isn't specific with regards to the consequences if S proceeded.

Taking these warnings individually and also collectively, I'm not satisfied that Starling provided specific, impactful warnings to S as required under the CRM Code. So, I'm not satisfied that Starling can fairly apply this exception as a reason not to reimburse S.

Did S have a reasonable basis for believing they were paying the person they expected?

The second reason Starling say they're not liable to reimburse S, relates to whether S had a reasonable basis to believe they were paying the person they expected.

In this case, I'm satisfied that S did have a reasonable basis for belief, and I'll explain why.

S had been dealing with a genuine university contact with regards to the course their employee was attending. At some point the emails between S and the university were intercepted by the fraudster and they changed the content of the emails being sent to S.

Having reviewed the intercepted emails S received, I'm not satisfied that there was enough about these that S should've realized they'd been altered.

The information provided in them included quite specific guidance around costs and information about the course, also the tone of the emails didn't significantly change. While the email address had changed it came up with the sender's name as a known contact, so didn't automatically show the whole email address. The name looked slightly different, but I think it's only with the benefit of hindsight and knowing it had been changed that it's obvious.

When S tried to make their first payment, they received a COP result which said the payee details didn't match the account holder information. This restricted the first payment S could make to only £1,000, which meant they had to make the second payment the following day.

S says it often sees a COP no match when making payments. They say it happens on genuine invoices on a regular basis, so they don't tend to be concerned when it happens. But S did take steps to confirm that the bank account information they were given were correct. Mr H called the university and tried to talk to the accounts team but was told that they weren't contactable by phone and that he should email them. Mr H says the call handler at the university also told him to refer to the details provided on the invoice.

The university later apologised to Mr H for the situation and confirmed that the accounts team were indeed working off site and weren't contactable by phone when he made this payment. So, the only way Mr H could've confirmed the bank details was through email, which was being controlled by the fraudster. I'm not persuaded that Mr H should've checked the university website for the bank account information, as he'd queried the details and been told the information on the invoice was correct.

Starling referred to S having previously paid the university with different account details, however that payment was several months before and S say they had no previous genuine invoices from the university – as the fraudsters accessed their emails and removed previous genuine emails.

From everything I've seen, I'm satisfied that S did enough checks, based on the information they had and in response to the COP no match – to satisfy themselves that they were paying the genuine university account. As I'm satisfied that they had a reasonable basis to believe they were paying the university, I'm not satisfied that Starling can rely on that exception as a reason not to refund S.

Having considered everything very carefully, I'm not satisfied that Starling has evidenced that they can fairly apply an exception to reimbursement. Therefore, Starling should refund S in full for both payments. Starling should also pay 8% simple interest on that refund, to account for S's loss of use of those funds. This should be calculated from the date Starling declined to refund S under the CRM Code, until the date of settlement.

Putting things right

To put things right Starling Bank Limited should:

- Refund S in full for both payments.
- Pay interest on that refund at 8% simple interest from the date they declined S's claim under the CRM Code until the date of settlement.

My final decision

My final decision is that I uphold this complaint against Starling Bank Limited and require them to compensate S as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask S to accept or reject my decision before 21 November 2022.

Lisa Lowe
Ombudsman