DRN-3431598

The complaint

Mr H on behalf of 'B', a limited company, complains that Starling Bank Limited ('Starling') declined to refund money which he says B lost as a result of an email intercept scam.

What happened

The details of this complaint are well known to both parties, so I will not go into every detail of what happened here. But in summary, in May 2021 Mr H made two payments totalling over £27,000 to a legitimate company he had contracted to complete some refurbishments to their salon. However, unbeknownst to Mr H or B, the funds were sent to a scammer who had intercepted the contractor's emails.

Mr H on behalf of B contracted a legitimate construction company to complete works on B's salon. The construction company were known to one of B's shareholders. They completed the works and invoicing and payment were organised. They liaised about payment over email, and agreed the cost would be split over three payments. The first was sent to the contractor's legitimate bank account. Mr H exchanged emails with the email address he had been corresponding with for some time, belonging to a person he had spoken to before, and another two email accounts. During these emails, Mr H was provided with two new bank account details for the two payments to be sent to. He sent the second and third payments to the new account details.

The scam came to light in June 2021 when the contractors contacted B to chase the two outstanding payments, and it transpired that an unknown third party had intercepted their emails and made Mr H send the payments to fraudulent accounts. Mr H raised the matter with Starling, the recipient banks and Action Fraud. Starling investigated B's complaint and issued its final response in July 2021 not upholding the complaint. In summary, they did not accept liability as they did not think Mr H on behalf of B had done enough to satisfy himself that he was sending the funds to the legitimate business. They also felt that he had ignored effective warnings about scams that were presented to him when he was trying to make the payments. They said they had contacted the bank of the receiving accounts, who were not liable. They were able to recover approximately £3,350 from the recipient accounts.

Unhappy with Starling's response, Mr H on behalf of B brought his complaint to our service and one of our investigators looked into what had happened. They recommended that the complaint be upheld in part. They felt that Mr H on behalf of B had not met the requisite level of care under the Lending Standard Board Contingent Reimbursement Model ('CRM code'). But they also said that the warnings Starling presented to Mr H at the time of the payments could not be considered effective warnings under the code. And so they recommended that each party share the liability, and so Starling would need to refund 50% of the losses to B, along with 8% simple interest from the date the claim was declined under the code to the date of settlement.

Mr H responded on behalf of B. He considered our investigator's view to have been a fair review of the events that had taken place, but disagreed with the overall conclusion that they could only recover 50% of the losses. He felt that the receiving banks should have done more to recover the funds and have done more to prevent fraudsters setting up accounts in the first instance.

Starling responded disagreeing with our investigator's findings with regard to effective warnings. They did not feel that all of their warnings had been taken into account. In summary, they said:

- Mr H was shown an initial warning both times about setting up a new payee which asked if this could be part of a scam, and warned of the potential outcome of not verifying who money was being sent to – that he may not be able to recover his funds. It invited him to visit their website for advice on scams.
- When asked the purpose of his first payment, Mr H said it was for a purchase. Starling said he should have selected their option for invoice or bill. Had he selected the correct option, as he did the second time, he would have seen the warning which he did at the time of the second payment.
- The warning displayed after invoice/bill said that fraudsters can take over email addresses or call from seemingly reputable numbers, posing as genuine organisations. It asked whether unexpected payments or payments to new accounts had been requested, and said to contact on a trusted channel separate from the one used to contact them. Starling said that this combined with the new payee warning should be judged as amounting to an effective warning.
- The warning for invoice/bill, when read in conjunction with the new payee warning, could be seen as an effective warning. Our investigator said that the warning was not effective because it did not warn about the possible consequences of ignoring the warning – the potential for the irreversible loss of funds. But they had already been warned about that when setting up the new payee.
- They agreed the warning could have been more concise in that it mentioned several different scenarios, but did not think this meant it was not effective. They said the language was sufficient and specific enough to help customers protect themselves.
- The investigator said that the second warning was one of the reasons they did not think Mr H had a reasonable basis for belief – which therefore Starling says means they must have been effective.

As no agreement could 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.

In deciding what's fair and reasonable in all the circumstances of the complaint, I'm required to take into account 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.

In broad terms, the starting position in law is that a bank is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of their customer's account. However, where the customer made the payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse them, even though they authorised the payment.

When thinking about what is fair and reasonable in this case, I have considered whether Starling should reimburse some or all of the money B lost in line with the provisions of the CRM Code it has agreed to adhere to and whether it ought to have done more to protect B from the possibility of financial harm from fraud.

There is no dispute here that Mr H was tricked into making the payments to the incorrect accounts. But this is not enough, in and of itself, for B to receive a refund of the money under the CRM Code. The Code places a level of care on B too.

The CRM Code

Starling is a signatory of the Lending Standards Board 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 say exceptions to reimbursement apply in this case. It says that Mr H on behalf of B didn't have a reasonable basis for believing the new account payee details he was given were from the legitimate company he transacted with. They also say Mr H ignored an effective warning.

It is for Starling to establish that a customer failed to meet a requisite level of care under one or more of the listed exceptions set out in the CRM Code.

Those exceptions are:

- The customer ignored an effective warning in relation to the payment being made;
- The customer made the payment without 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.*

Did Mr H, acting on behalf of B, ignore an effective warning in relation to the payment being made?

Under the provisions of the CRM Code, as a minimum any 'effective warning' needs to be understandable, clear, timely, impactful and specific. It must also provide information that gives customers a better chance to protect themselves against being defrauded and should include appropriate actions for customers to take to protect themselves from APP scams. In short – the warning needs to be capable of countering the typical features of the generic scam type identified during the payment journey.

Each time Mr B set up a new payees, he was presented with a warning which read:

> "*Could this be part of a scam? Always verify who you are sending money to as you may not be able to recover these funds. A fraudster may tell you to ignore these warnings. Visit our website for scam advice."*

When making the payments, Mr H was asked the purpose of each payment in turn. For the first payment Mr H selected the option to say he was sending the payment to make a purchase. Starling have asserted that he should have selected the option for bill or invoice here. Based on this choice, he was presented with the following warning:

> "*THINK BEFORE YOU SEND*
> - *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 or if you do not know the seller, check the reviews online before you buy*
> - *Have they asked you to pay quickly or requested payment via bank transfer instead of by card or PayPal?*
> - *If you have any concerns, stop the payment now or pay by card, which provides you with more protection.*
> - *Fraudsters are currently claiming to sell in-demand items such as face masks, hand sanitizer and Coronavirus testing kits.*
>
> *Could this be linked to a Coronavirus scam?*
> *Visit the website to learn more about how to protect yourself from fraud."*

Starling have not argued that this represented an effective warning in this case, but instead have suggested that the warning they presented for the invoice or bill option was effective, and that Mr H should have selected this option for both payments. The warning for this read as follows:

"THINK BEFORE YOU SEND

- *Fraudsters can take-over email addresses or call from seemingly reputable numbers, posing as genuine organisations.*
- *Have you been asked to make an unexpected payment to a new account?*
- *Have you been told that the account details for a payment have changed recently?*
- *Check any unexpected or amended instructions via a trusted channel that is separate to the one that they used to contact you.*
- *HMRC scams are common, and fraudsters have used the current Covid-19 pandemic as an opportunity to target people, posing as HMRC via SMS or email. Contact HMRC directly via contact information on their website or login to their online services if you have been contacted by them.*
  Visit the website to learn more about how to protect yourself from fraud."

Mr H has not been able to say exactly why he chose 'purchase' as the reason for the first payment, but given that he was paying for goods and services of the contractors, I do not think this was unreasonable in the circumstances. I do agree with Starling that the payment reason was more closely aligned to the bills and invoices option. Nevertheless, I do not agree with Starling that the warning given when Mr H selected the 'correct' payment method was effective in the circumstances. So, I don't think whether Mr H selected the 'correct' reason or not has a material difference here. I'll explain why.

The warning for invoices and bills did talk about the fact that emails and phone numbers could be spoofed. Whilst this warning does mention the possibility of fraudsters impersonating a professional contact, as they did here intercepting B's emails, I do not think it goes into enough detail about what the scam could look or feel like or is specific enough to be effective at bringing the scam to life in B's circumstances. I think the references to HMRC, Coronavirus scams and unexpected bills can reasonably water down the impact of the warning. And whilst when setting up a new payee Mr H was warned about the potential impact of sending money to a fraudster, I think because this took place in a different process (setting up the new payee rather than making the payment), it again loses some of the impact that a more specific warning including potential consequences of continuing with the specific payment would.

I don't underestimate the challenge Starling faces in providing warnings strong enough to break the spell in a sophisticated scam such as this. But the difficulty of meeting that challenge does not mean the warnings given by Starling were sufficient or contained enough clarity to meet the minimum requirements in the CRM code. Overall, I am not satisfied that the warnings met the requisite criteria here. I don't consider the warnings given were effective warnings as defined within the CRM code. It follows that Starling has not established it can fairly apply the exception to reimbursement relating to Mr H 'ignoring an effective warning'.

Did Mr H, acting on behalf of B, have a reasonable basis for belief?

Starling have asserted that Mr H should have carried out further checks before making the payment and that, if he had done the checks suggested in the warning he was shown, the scam could have been prevented. In response to our investigator's view, Mr H did appear to accept that he could have done more to ensure he was paying the correct accounts on behalf of B. But, for completeness I will summarise the reasons why I agree with our investigator on this point here.

- Having reviewed the lengthy email chain, the emails from the scammer(s) were materially different. This included a change of email address (going between the hacked account and two different email addresses), a change of name of the person they were speaking to at the company, a change of tone and professionalism, as well

as containing more spelling and grammar errors. The tone certainly also felt pushier with regard to securing payments. Whilst this in and of itself ought not to have given reason not to proceed with the payments, I think in conjunction with other warnings that I will go on to describe, it should have alerted Mr H to the possibility of something not being legitimate here.

- Internal policy at B said that new payee details required verification before payments were processed when they came from an unknown source. One set of payment details came from a different email address. I do appreciate the email was written in a way to appear like the genuine company email addresses but was actually distinctly different and from a person with a different name. So, according to B company policy this should have been verified – which it was not.
- When making one of the payments, the 'confirmation of payee' process flagged that the account name did not match the one Mr H had entered. He quite rightly spoke to who he thought were the contractors over email, who told him to put a different, personal name in the account name box. Mr H did not query at this point who this was, or why a business payment was being sent to a personal account, or why the name was not one he had heard before as associated with the contractors.
- Before the final payment was sent, Mr H was told he needed to pay a contractor account and was given a new set of personal account details, in another name. As with the first scam payment, this was not a name which would have been known to Mr H or B as someone associated with the contractors. And Mr H said the contractors completed the work themselves, they did not hire any sub-contractors. So I think this ought to have given Mr H and B cause for concern, which should have led to him questioning the legitimacy of the details he had been given.
- Whilst I concluded that the warning for invoices and bills was not sufficient to be considered 'effective' under the code, I do think reading it should have given Mr H some cause for concern when combined with the other factors I have talked about here. It did let him know that sometimes legitimate email addresses could be hacked, and that it would always be appropriate to contact someone you are expecting to pay through another legitimate method of communication before proceeding with a payment. It is unclear why Mr H did not follow the advice contained within the warning, and telephone the contractors before proceeding with the sizable payment.

I have considered all of this against the standard of the average person and their financial understanding – but it is also worth noting here that Mr H acted as B's financial controller and so I would expect a higher level of financial awareness than the average person. This does not mean he would be more aware of fraud or scams in particular, but to have a better knowledge of payment processes, general way of reducing the risk of fraud, business operations, and the difference between business and personal accounts – and internal company policy. He was, after all, the financial controller who was in charge of dealing with large sums of company money.

So on balance, I am satisfied that when considering all of the circumstances, Mr H's decision on behalf of B to make the payments without further checks such as calling the contractors, can not be seen as reasonable in the circumstances. Mr H on behalf of B should have been alive to the possibility he was dealing with a fraudster. With this in mind, and in line with the CRM code, I am satisfied that Starling has been able to establish that Mr H on behalf of B sent the payments without a reasonable basis for belief.

Should Starling have done more to protect B?

In addition to their responsibilities under the CRM code, when Mr H made the payments on behalf of B Starling should fairly and reasonably have had systems in place to look out for unusual and out of character transactions or other signs that might indicate that B was at risk of fraud or financial harm (amongst other things).

Whilst the payments were for large sums of money, they did not stand out as sufficiently unusual that I think Starling ought to have stopped them or contacted B. This is because they did not stand out compared to other similar payments on the account.

Recovery

I have also considered whether Starling could have done more to try to recover the money once they had been told of the scam. We would expect a business to take reasonable steps to try and recover the money from the bank it was sent to, with urgency, after their customer notifies them they fell victim to a scam. Starling did try to recover the funds B sent to the scammer within an appropriate amount of time – and were able to evidence that they contacted the receiving bank within less than an hour after Mr H contacted them. They were unfortunately only able to recover approximately £3,350 as the other funds had been removed from the accounts. So I don't think Starling could have done more to recover Mr B's funds here.

Putting things right

The Code explains that where a customer has not ignored an effective warning, but has also not met their requisite level of care (which as I have explained, I am satisfied was the case here) they should share the liability with the bank in question. So I think it is fair that Starling should:

- Refund 50% of the two payments minus the £3,350.59 it has already recovered.
- Pay an additional 8% simple interest on this refund, calculated from the date the claim was declined under the CRM to the date of settlement.

My final decision

I uphold this complaint in part and ask Starling Bank Limited to refund B in line with what I explained above. Starling must pay the compensation within 28 days of the date on which we tell it that B accepts my final decision.

*If Starling Bank Limited deducts tax from the interest element of this award it should provide B with the appropriate tax certificate so it might submit a claim to HMRC if applicable.

Under the rules of the Financial Ombudsman Service, I'm required to ask B to accept or reject my decision before 4 August 2023.

Katherine Jones
Ombudsman