DRN-3534272

The complaint

A company, which I'll refer to as B, complains that Worldwide Currencies Limited ('WCL') won't refund the money it's lost to a scam.

Mrs T, who is a director of B, brings the complaint on B's behalf.

What's happened?

B has fallen victim to an email interception scam.

On 4 June 2020, Mrs T sent WCL an email asking it to pay a total of $66,458.23 to an international account held by one of B's regular suppliers ('the supplier'). She provided new account details for the supplier, which she had received via email. Unbeknown to her, the supplier's email account had been hacked, and the hacker had sent the new account details – which weren't really for an account held by the supplier.

WCL instructed a third-party bank to send B's money to the nominated account.

When the fraud came to light, Mrs T complained to WCL. She said that it failed to take reasonable steps to protect B from financial harm.

WCL's response to B's complaint

WCL has said that it is its policy, when it receives a new payment instruction or a request to amend a payment instruction via email, to call its customer and confirm the payment instruction received is legitimate and correct. This is to help prevent fraud by email interception.

So, when WCL received Mrs T's email on 4 June 2020, it emailed her asking her to call and confirm the new account details and verify the name on the nominated account (as this was missing from the payment instruction). WCL's email said: *"Could you please call me back so I can confirm the new bank details with you and also can you please e-mail back the account name please*?"

In response to its emails, WCL says Mrs T called it and verified the account number, and she was asked if the account name had also been verified. She said she would check with the supplier, and she called back later the same day to confirm that she had done so. The payment she had instructed was then made.

WCL says that, in later calls, Mrs T confirmed to it that she had been asked to double-check the new account details with the supplier, but when she called the supplier, she only asked for the account name and did not mention the new account number. So, although WCL asked Mrs T to assure herself of the new account details by calling the supplier, she failed to make adequate checks. B is responsible for providing WCL with accurate information, in accordance with the terms and conditions of its account.

WCL took immediate action to try and recover the funds B lost to the fraud. But unfortunately, no funds have been recovered.

What did our investigator say?

Our investigator wasn't persuaded that WCL asked Mrs T to check the new account number with the supplier. And, in any event, they thought that WCL missed an opportunity to prevent the fraud by asking Mrs T probing questions about the payment she had instructed and giving her relevant warnings about email interception scams.

Our investigator recommended that WCL reimburse the $66,458.23 transaction and pay B 8% simple interest from the date of the transaction to the date of settlement.

WCL's response to our investigator

WCL did not accept our investigator's assessment of B's complaint. In summary, WCL said:

- The email WCL sent Mrs T on 4 June 2020 shows an intention to check the new account details and name. There is no proof that WCL did not do so in the call that took place later that day, and it questions why our investigator would conclude it is more likely than not that it didn't do so. WCL maintains that it did ask Mrs T to check the new account details and name with the supplier, and it says that, just because Mrs T did not follow its instructions, it cannot be assumed that the instructions were not given.

- The email of 4 June 2020 is evidence that Mrs T was asked to check the new account name and number with the supplier.

- Mrs T confirmed that WCL asked her to verify the account details with the supplier in a call that took place on 17 August 2020. It was only in a call that took place on 20 August 2020 that she admitted she didn't check the new account number with the supplier. When she admitted to not checking the account number, she didn't say it was because she wasn't advised to do so, she said she didn't because she had the account number on what she thought was a genuine email, so she just asked for the account name which was missing.

- WCL asked Mrs T probing questions about the payment she'd instructed on 4 June 2020, and it gave her sufficient fraud warnings. WCL said that the supplier's bank details hadn't changed before and this was suspicious, and it advised Mrs T to call the supplier and double-check the details because there's a lot of fraudulent activity going on and she needs to keep her wits about her. So, WCL acted reasonably at the time and Mrs T failed to make adequate checks with the supplier.

- The relevant transaction was authorised.

- B is a company and Mrs T is experienced in business, yet our investigator has held WCL to a higher standard of care than B/Mrs T.

- There is no evidence that B has suffered a financial loss as a result of the fraud. In a call which took place on 20 August 2020, Mrs T told WCL that B wasn't out of pocket as she'd held onto the stock she'd attempted to pay for.

The complaint has now 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.

I won't be addressing every argument that has been put forward by the parties, of which there have been many, but no disrespect is intended. It doesn't follow that I haven't considered every argument, I simply don't need to address each point in reaching an outcome I consider to be fair and reasonable. I have concentrated on the issues that I think are central to the outcome of this complaint.

It is not in dispute that the relevant transaction was authorised, and that WCL had an obligation to follow B's payment instruction. But that's not the end of the story. Taking into account regulator's rules and guidance and what I consider to have been good industry practice at the time, I consider that WCL owed a duty of care to protect its customers against the risk of fraud and scams so far as reasonably possible.

I accept that B is a company, and Mrs T may be experienced in business, but it doesn't follow that B or Mrs T should reasonably possess any special knowledge of email interception scams. Firms are generally more familiar with fraud and scams than their customers, and I would expect firms to be taking steps to protect their customers from the risk of harm from fraud.

WCL's fraud prevention policy says:

"New Payee instructions
To ensure our clients emails have not been intercepted, when we receive a new payment instruction or a request to amend a payment instruction via email, we always call the client on a registered contact number and confirm that the payment instructions received are legitimate and correct."

From this, I am satisfied that WCL was aware of email interception scams and their common features, and that WCL can reasonably be expected to take steps to protect its customers from email interception scams where a scam risk is identified.

WCL noticed that Mrs T had provided new account details for the supplier, and it made contact with her about this. The question for me to decide is whether WCL did enough to protect B from financial harm.

Unfortunately, WCL hasn't been able to provide recordings of the telephone conversations it had with Mrs T on 4 June 2020, and it hasn't provided any contemporaneous contact notes in relation to the calls either. It's not in dispute that the telephone conversations took place, but the parties don't agree on what was said. WCL has said that other evidence it's been able to provide shows what was said during the calls, but I can't agree. WCL's fraud prevention policy sets out that it should call clients when it receives a new payment instruction or a request to amend a payment instruction via email, to check that the payment instruction received is legitimate and correct and ensure the clients email hasn't been intercepted. I think the email WCL sent to Mrs T on 4 June 2020 is evidence of it following this policy. But it only shows that WCL asked Mrs T to confirm the supplier's new account details with it, not that WCL went on to advise Mrs T to check the new account details with the supplier. And I've listened to call recordings of the conversations that took place between WCL and Mrs T on 17 and 20 August 2020, but I didn't hear Mrs T confirm that she was advised to check the new account number with the supplier over the telephone as WCL says she did. There's reference to reading out the new account number in the call of 17 August 2020, but I don't think it follows that WCL asked Mrs T to read the new account number out to the supplier when it spoke to her on 4 June 2020 – it could just be that's what WCL expected Mrs T to do, without specifically advising her to do so.

In the circumstances, I must draw conclusions based on the balance of probabilities – that is to say, what I think is most likely to have happened.

Mrs T says that WCL asked her to call the supplier and check the name on the new account, because that was missing from her payment instruction, and that is what she did. WCL says it advised Mrs T to check the new account details and name with the supplier. Given that Mrs T did make a call to the supplier and asked for the account name, I think it's most likely that she would've checked the new account number too if she'd been clearly advised to do so – particularly if the scam risk had been made clear to her. I don't think it's likely she would've taken steps to follow WCL's instructions by contacting the supplier but neglected to check all of the details WCL had clearly advised her to check. So, I'm persuaded that it's most likely WCL either didn't advise Mrs T to check the new account number with the supplier, or it didn't clearly advise her to do so.

In any event, I haven't seen evidence from either party that WCL asked Mrs T appropriate questions about the payment or sufficiently educated her about email interception scams as I would've expected it to do. WCL knew that the account details of a regular payee were changing, and in the arguments it has made, WCL has made it clear it was aware that this is a common feature of email interception scams. Mrs T wasn't being coached by the fraudster, so I think she would've spoken freely to WCL. If it had asked her some probing questions about the payment, I think it would most likely have become apparent that she'd received the new account details via email (if it wasn't clear, and there's a suggestion in the arguments WCL has presented that it was). WCL ought to have given Mrs T information about the prevalence of email interception scams and the risk of receiving payment details in the way she had. If WCL had brought the common features and risks of this type of scam to Mrs T's attention, she'd have had the knowledge she needed to adequately protect B from the scam. She's said she would've checked the new account number with the supplier if WCL had sufficiently educated her about email interception scams, and I think that's likely – particularly as she did contact the supplier at WCL's request. Had Mrs T checked the new account number with the supplier, as I think she would've, I think the scam would've quickly unfolded and B wouldn't have gone ahead with the payment.

But Mrs T says the risk of harm from fraud was not brought to her attention on 4 June 2020. The conversation between WCL and Mrs T which took place on 20 August 2020 appears to support this – it seems like the first time the parties discussed how email interception scams work, and Mrs T tells WCL that, as far as she knew, the email came from the supplier. She says she just thought she needed to request the account name from the supplier as this was missing from her payment instruction.

WCL has said it told Mrs T that the supplier's bank details changing was suspicious, and it advised Mrs T to call the supplier and double-check the details because there's a lot of fraudulent activity going on and she needs to keep her wits about her. But I don't think this is sufficient warning because it doesn't bring to life how email interception scams work – it doesn't explain, for example, that scammers will often request payment of invoices to new account details and that their emails often appear genuine and look like they come from the correct email address. An instruction to check the new account details with the supplier is somewhat meaningless without context because it doesn't explain why the new account details needs to be checked or fully equip the recipient with the knowledge required to protect themselves from financial harm.

Overall, I think that WCL should've asked Mrs T appropriate questions about the payment and given her sufficient information about how email interception scams to enable her to protect B from financial harm. If it had done so, I think the fraud would've been prevented and B would not have suffered a financial loss. So, I think the fair and reasonable outcome here is to uphold the complaint and require WCL to reimburse B.

WCL has suggested that B may not have suffered a financial loss in this case, because it received the stock it intended to pay the supplier for when it was defrauded. But, from what I've seen, I'm satisfied that it has. Mrs T has shown that B has gone on to pay the supplier $20,000 towards the relevant invoice, and that the rest of the debt remains owing to the supplier for payment in the future. So, B has received the stock, but it owes the supplier for that stock, and it has lost the money it intended to pay the supplier with to this scam.

B owed the supplier the $66,458.23 that was paid to the scammer. So, but for the fraud, B would not have had use of that money for other things or had the opportunity to earn interest on the money. But B has paid the supplier $20,000 towards the relevant invoice that it wouldn't have needed to pay if it hadn't been defrauded. B would have had the extra $20,000 available to spend on other things, but I can't know what that money would've been spent on. So, I think it's fairest to award 8% simple interest per annum on the extra $20,000 B would have had available to spend from the date it paid this amount to the supplier (8 January 2021) to the date of settlement.

Finally, I have considered whether B should bear some responsibility for its loss by way of contributory negligence. But I don't think it should. Mrs T received an email which appeared to come from the supplier. And she contacted the supplier to obtain the extra information she thought WCL needed to process the payment. I've concluded that WCL didn't sufficiently educate Mrs T on the type of fraud concerned. Overall, I'm persuaded that Mrs T did not realise anything was amiss when she instructed the relevant payment, and I think that was reasonable in the circumstances. She was the unwitting and blameless victim of a sophisticated scam.

My final decision

For the reasons I've explained, my final decision is that I uphold this complaint and instruct Worldwide Currencies Limited to:

- Reimburse the $66,458.23 that B lost to the scam; and
- Pay 8% simple interest per annum on the extra £20,000 B would have had available to spend from the date it paid this amount to the supplier (8 January 2021) to 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 20 February 2023.

Kyley Hanson
Ombudsman