

The complaint

K, a limited company, complains that Smart Currency Exchange Limited won't refund the money it lost when it was the victim of a scam.

What happened

K is a limited company and, in April 2021, it contacted Smart Currency Exchange Limited (SCE) to arrange the payment of invoices to two foreign suppliers. K and SCE agreed a contract for the payment of the invoices and SCE emailed K confirming where K should send the money for the payment and asking it to confirm the details of the invoices to be paid.

K then emailed copies of the invoices and details of the bank details for the suppliers to SCE. But it appears that K's emails had been compromised and scammers were able to intercept this email and send a fake email to SCE, with a fake invoice and different bank details for one of the suppliers. SCE called K to check the payment details and K said to check the payment details matched the invoices it had sent. SCE then made the payments in line with the invoices it had received, and so one of the payments – for €18,068, was made to the bank details the scammers had emailed to SCE, rather than the details K had intended.

The scam was uncovered after one of the suppliers told K it hadn't received the payment for the invoice. K asked SCE to confirm the bank details the payment had been sent to and it was discovered the bank details didn't match those on K's original invoice. K had to make a second payment to the supplier, and complained to SCE about the scam and asked it to refund the money it had lost.

SCE investigated K's complaint but said it had made the payment in line with the instructions it had received and had checked the payment details with K before making the payment. So it didn't agree it had acted unfairly and didn't agree to refund the money K had lost. K wasn't satisfied with SCE's response, so referred its complaint to our service.

One of our investigators looked at the complaint. They felt SCE should have done more to try to avoid the risk of the scam and that, if it had done so, K wouldn't have lost the money. So they felt SCE should refund the money K lost. SCE didn't agree with our investigator, so the complaint has been passed to me.

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 a 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 payment service provider is expected to process payments that a customer instructs it to make. And a customer will then be responsible for those transactions that they have authorised.

But the regulatory landscape, along with good industry practice, also sets out a requirement for payment service providers to protect their customers from fraud and financial harm. And this includes monitoring transactions to look out for activity that might suggest a customer was at risk of financial harm, intervening in unusual or out of character transactions and trying to prevent customers falling victims to scams. So I've also thought about whether SCE did enough to try to keep K's money safe.

SCE called K to check the payment details were correct, so there was a direct interaction between K and SCE and a clear opportunity for SCE to ask questions before processing the payment. SCE has said that, where it receives payment details by email, it will then call the customer to confirm them before making the payment – and it appears that this is done, at least in part, to combat the risk of incorrect payment details being given in the email.

But having listened to the call between SCE and K, I don't think SCE asked clear enough questions or explained the risks to K clearly enough to address this risk. In the call, SCE says it needs to confirm the payment details over the phone. But it doesn't then read out or confirm any of the details it has or ask K to confirm the details from another source, such as the original invoice. It didn't explain the possible risks of invoices being intercepted or incorrect payment details being given and it didn't give any examples of steps K could take to avoid these risks. And it accepts K just asking it to use the payment details from the email. And if a customer can just ask to use the payment details from the email, I can't see that the call to confirm the details serves any real purpose. So, having made the phone call to confirm the payment details, I think SCE should have done more in this call to help protect K.

If SCE had explained the possible risks or asked K to confirm the payment details from another source, as I think it should have done, I think the scam here would have been uncovered and the money wouldn't have been sent to the incorrect details. And so I think SCE should refund the money K lost as a result of this scam.

My final decision

For the reasons set out above, I uphold this complaint and require Smart Currency Exchange Limited to:

- Refund K the €18,068 it lost as a result of this scam
- Pay 8% simple interest on that refund from the date of the payment until the date of settlement

Under the rules of the Financial Ombudsman Service, I'm required to ask K to accept or reject my decision before 30 December 2022.

Alan Millward
Ombudsman