DRN-5617248

The complaint

Mr H brings this complaint on behalf of M, a limited company. His complaint is that Currencies Direct Limited hasn't reimbursed M after it fell victim to a scam.

Mr H had authority to act on behalf of M and so for ease I will refer to Mr H throughout the decision.

What happened

On 5 February 2024 Mr H entered into a contract with Currencies Direct to sell around £200,000 and purchase the equivalent in Euros. He instructed Currencies Direct to then send the Euros to a beneficiary abroad. It appears over the phone he provided the payment details – "IBAN A", "bank A" and "SWIFT code A".

Mr H emailed Currencies Direct at 9:51 am on 5 February 2024 confirming the payment details above. Later the same day Mr H said scammers sent an email from his email account updating the payment details. They provided "IBAN B", "bank B" and "SWIFT code B".

It appears two more emails were sent the same day. One at 6:10pm providing IBAN B and SWIFT code A and one at 6:15pm providing IBAN B and SWIFT code B.

On 8 February 2024 Currencies Direct called Mr H and as part of this call it asked him to read out the beneficiary's bank details. Currencies Direct told him it had 'several', so it wanted to ensure it would be using the correct account. Mr H provided IBAN B, bank B and SWIFT code A during this call – a combination of the details he originally provided and the ones he's said scammers provided.

On 9 February 2024 at 1:03pm Currencies Direct emailed Mr H again to confirm it had the correct details, it provided IBAN B, and bank A. At 1:37pm scammers responded from Mr H's account and said the bank should be bank B and provided SWIFT code B unprompted.

On 9 February 2024 at 2:19pm Currencies Direct contacted Mr H and advised the IBAN number it was using – seemingly the correct IBAN A - was returning SWIFT code A and bank A and again asked Mr H to confirm the correct details. A response from Mr H's account was sent at 2:37pm confirming bank A and B were the same bank but changed the SWIFT code to SWIFT code B – the scammer's SWIFT code.

On 16 February 2024 the beneficiary's bank rejected the payment due to an issue with the SWIFT code. Currencies Direct contacted Mr H by phone to ask for confirmation of the SWIFT code. Mr H tried to call back to confirm, but couldn't get through. So he sent an email at 2:26pm to confirm the payment should be using SWIFT code A (the IBAN was not corrected in this email). However, this email wasn't delivered to Currencies Direct because the email address Mr H used was incorrect and so it wasn't delivered.

Currencies Direct did, however, receive an email later that day from Mr H's email account at 15:01 to confirm Currencies Direct was using the correct SWIFT code – SWIFT code B – but

"XXX" needed to be added to the end. Currencies Direct then used the details it had been given– IBAN B and SWIFT code B – to make the payment.

On 26 February 2024 Mr H contacted Currencies Direct as the beneficiary hadn't received the funds. He called the following day to confirm he'd discovered he'd been the victim of a scam. Currencies Direct contacted the beneficiary's bank the same day to try and recover the funds. The beneficiary bank did initially acknowledge this contact but later stopped responding and the funds weren't recovered.

Mr H said he had been the victim of an email intercept scam. He's said the payment wasn't authorised by him as scammers had accessed his emails and provided the payment instruction that was used to Currencies Direct.

I issued my provisional decision on 7 August 2025 I said that:

In cases like this it will never be possible for this service to determine exactly what has happened. It's the case that evidence and information will often be incomplete. I must use what is available to reach what I consider to be the fair and reasonable outcome in all the circumstances of the complaint. In doing so I will reach my findings on the balance of probabilities. And where there is a dispute, I'll use the available evidence to decide what I consider is more likely than not to have happened.

Were the transactions authorised by M?

The starting point at law is that a customer is responsible for any transactions made from their account which are properly authorised. This is set out in the Payment Service Regulations ("PSRs") and confirmed in Mr W's account terms and conditions.

Where there is a dispute over the authorisation of payments, as there is here, a firm must be able to evidence that it is more likely than not the customer made or otherwise authorised the payments. There are two important parts to authorisation – authentication and consent. I'll address each separately.

For the authentication of the payment instruction I'd expect Currencies Direct to show that M gave the payment instructions in line with the terms and conditions of the account and I'm satisfied it has done that here.

It isn't in dispute that Mr H is authorised to give instruction on behalf of M – the limited company that is Currencies Direct's customer. And Currencies Direct's terms and conditions set out that it is entitled to act on instruction received by email which are, or reasonably appear to be from an authorised person.

In this case I'm satisfied the instructions came from what reasonably appeared to be an authorised person, and I've said more about this below. So as a starting point, overall, I'm satisfied that Currencies Direct has demonstrated that the payment was authenticated in line with the PSRs and the applicable terms and conditions.

The question of consent requires further consideration and is the crux of the issue here. Mr H has said that whilst the payment instruction might've come from his email address, and therefore was correctly authenticated, he didn't consent to the payments as the payment details used were provided by scammers who were acting without his consent. So it wasn't authorised.

I've considered all of the available information in this case very carefully. But overall, I'm not persuaded Mr H didn't consent to the payment instruction. Because of this I think it's more

likely than not the payment was authorised by M and therefore M is liable for it. In reaching this conclusion I've taken the following into account:

- *Currencies Direct has provided evidence to support that emails Mr H says were sent by the scammer, came from the same IP address and in some cases the same device Mr H has previously used to contact it. Mr H has said scammers must've somehow altered this, but this isn't consistent with how the type of scam he's described tends to be perpetrated. So it's not clear how someone, without Mr H's authorisation or knowledge would've been able to access his device, or devices on his usual network. We've asked him about this, and he hasn't been able to provide any information or plausible explanation for this.*

- *On 8 February 2024 Currencies Direct called Mr H to confirm which payment details to use. It said it had received "several" different accounts and wished to confirm. During this call, Mr H provided IBAN B, bank B (the scammer's details) and SWIFT code A (the correct code). It's not clear why Mr H provided details he's said were provided by the scammer during this call. We've asked Mr H about this, and he hasn't been able to explain why these details were given.*

- *Mr H confirmed during this call that he was looking through his emails to find the correct details, so I accept he may well have mistakenly read out an email the scammer had sent. But it seems unusual the scammer would've confused the two sets of payment details by sending the genuine SWIFT code but the scammer's IBAN. It also seems odd that when searching through his emails, Mr H didn't notice there were numerous emails with payment details provided. And it's clear the emails were still available to Mr H, because he later provided them to our service. Some of them also appear in email chains Mr H seems to have used to respond to Currencies Direct regarding requests for documents as part of Currencies Direct's due diligence checks.*

- *It's also not clear why, during this call, Mr H didn't find it odd that Currencies Direct said it had received 'several' different accounts to make the payment in question to. According to his testimony he wouldn't have expected this to be the case, so it's not clear why he wouldn't have been concerned by this.*

- *On 16 February 2024 after the payment was rejected, Currencies Direct contacted Mr H again by phone to clarify the correct details. Mr H was seemingly unable to confirm the details at that time and said he would call back. He was audibly frustrated during this call that Currencies Direct hadn't already made the payment. When he called back the relationship manager was unavailable so Mr H decided to email instead. But the email he sent was sent to the wrong address. It seems it was typed out manually and an extra 'i' was included in the word 'currencies' in the domain name. And this seems unusual. It's not clear why Mr H would've chosen to manually type the email address on this occasion given it had likely been stored in his email account or he could've replied to the ongoing email chain he'd previously used. It's also not clear why Mr H wouldn't have received or noticed a notification from his provider that the email had not been delivered, given it appears unlikely that the incorrect email address, which mis-spelt the word 'currencies', exists.*

- *Mr H has suggested that the scammers, as well as using his email account to send emails that appear to come from him, may have changed the outgoing email address stored on his email account to prevent his emails reaching Currencies Direct. And so it's not the case that he typed out the incorrect email address in full, he thinks he selected a contact name and the scammers had changed the email address. Mr H hasn't provided any evidence to support this. And if scammers had done this, it's not*

clear why this wouldn't have impacted other emails Mr H says he did send to Currencies Direct.

Overall, I don't think Mr H has been able to provide sufficient evidence to support that his email account has been accessed by scammers. It seems there have been several attempts by Currencies Direct to verify some of the information it had received from Mr H and it's unfortunate that at every point in the process something went wrong that meant Mr H wasn't alerted to any issues with the situation as I would've expected him to have been based on his testimony. This would've required scammers to have had near constant access and oversite of Mr H's account, IP address and at times device.

I think that overall it seems strange that Mr H doesn't seem to have been concerned or to have looked more closely into why Currencies Direct was having difficulty in establishing the correct account to send the money to.

I'd also add that the situation Mr H has described doesn't align with what we would typically see with email intercept scams. It's unusual that a scammer would direct a banking services provider to send the payment to the wrong beneficiary, rather than a consumer. I say this because a banking service provider would have more expertise around how scams tend to be perpetrated and the risk of the scam being uncovered would potentially be greater.

Taking everything into account overall, I haven't seen sufficient evidence to persuade me that it's more likely that not Mr H didn't authorise the payment in this case. So Currencies Direct is acting fairly in holding M liable for it.

I understand Mr H has raised concerns that Currencies Direct should've done more to spot irregularities in the correspondence and the situation he's described. He's suggested that the scam would've been uncovered if it had. As I've concluded the payment was likely authorised by Mr H, who had authority to act for M, I'm satisfied the payment has been sent to the account Mr H directed it was sent to. So I don't think there was anything here for Currencies Direct to prevent or uncover.

Mistakes can be made even when a payment has been authorised and so Currencies Direct did what I would've expected when it was alerted to the fact the money had been sent to the wrong account and contacted the beneficiary's bank. The beneficiary's bank stopped responding to Currencies Direct so it was unable to establish if the funds could be recalled. I'm satisfied it's done what I would've reasonably expected in trying to recall the payment. Unfortunately, it has no control over whether the receiving bank is co-operative in situations like these.

Currencies Direct accepted the decision and had no further comments. Mr H didn't and asked me to take some further considerations into account which I've summarised below:

- He felt Currencies Direct had missed clear warning signs that Mr H had been the victim of a scam and raised concerns over its security processes and how it actions payments.
- He said whilst he found it strange Currencies Direct said it had received several payment details, he knew he'd sent the correct details so felt assured the payment would be correctly sent.
- When he provided the incorrect details over the phone, it was due to searching for

previous emails on his phone and not realising these details had been sent by the scammer.
- He said he hadn't seen emails from the scammer until Currencies Direct started its investigation into the disputed transaction.
- A later payment of around 130,000 euros was sent to the correct recipient without the need for Mr H to confirm the right details. He's questioned how this happened.
- He didn't believe Currencies Direct did enough to try and recall the funds because it didn't contact the beneficiary bank directly, it contacted its intermediary bank instead.
- He was unable to offer an explanation as to how someone could access his device and communicate from his IP address. But questioned why, if someone had this kind of access, they wouldn't have taken more from M.
- He maintained the scammer must've changed Currencies Direct's email address in his stored contacts which is why one of his emails didn't go through.

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've considered everything Mr H has said very carefully and I have looked at the case again. But my findings remain the same as set out in my provisional decision above. There are some points I have responded to in more detail here, but if there's something I haven't addressed specifically it's because I have no further comment beyond that provided in my provisional decision.

Mr H's response is largely about what he views as Currencies Direct's failings in the way it manages and actions payments, and the various points at which he feels it ought to have recognised Mr H had been the victim of a scam and intervened.

I understand Mr H's strength of feeling. But the issue for me to decide in this case is whether I think Mr H likely authorised the payments based on the evidence available. As I'm satisfied he likely did authorise the payments, I'm satisfied Currencies Direct followed his instructions correctly. So there wasn't anything for it to uncover here.

I explained in my provisional decision why, on balance, I felt it was more likely Mr H had authorised the payment, but there are some points he addressed further and that I'd like to respond to.

Mr H has said he can't explain how emails he said the scammer sent came from his IP address. He's suggested this may not have been the case. But based on the evidence I've seen I'm satisfied the emails Mr H said were sent by scammers have likely been sent from the same IP address he's sent emails from in the past.

Based on what we currently know about this type of scam and how it tends to be perpetrated, I don't think there is a plausible explanation as to how emails Mr H says were sent by scammers were sent to Currencies Direct from his genuine IP address without his knowledge or consent.

I don't think Mr H has been able to explain in his response to the provisional decision why he didn't recognise emails in his email account he says weren't sent by him. Whilst he's said he didn't have the emails until the investigation into the disputed payment, this doesn't seem plausible given he's also said he mistakenly read one out to Currencies Direct when it called him to confirm the correct payment details.

I also don't think Mr H's comments in response to the provisional decision explain his actions when Currencies Direct told him it had several bank account details and wanted to confirm the correct one. He's said he did find this strange, but doesn't appear to have asked for any clarification around this or to have looked into this any further. And whilst he's said he didn't worry in part because he knew he'd sent the correct details, it's not clear why it wouldn't have concerned him more that someone had unexpectedly provided different payment details on his behalf.

Mr H has said Currencies Direct didn't contact the beneficiary's bank in this case, it contacted its intermediary bank. He's said he's aware the beneficiary's bank initially responded to the intermediary. Mr H has expressed his concerns there aren't greater obligations on international banks to respond to this type of claim. But in terms of what I'm deciding in this case, I'm satisfied Currencies Direct took reasonable steps in trying to recall the funds. The fact that this wasn't possible was beyond its control.

I've noted Mr H's comments that a later payment of around 130,000 euros was sent to the correct recipient without any further intervention from him. So he's said it's clear Currencies Direct must've stored the correct payment details and used them later. What I've had to decide in this case is whether I think Currencies Direct is liable for the payment Mr H is disputing. As I'm satisfied he likely authorised the payment, I don't think it is. I don't think the fact it later made a payment Mr H has not disputed changes this.

My final decision

I don't uphold this complaint. Under the rules of the Financial Ombudsman Service, I'm required to ask M to accept or reject my decision before 30 September 2025.
Faye Brownhill
Ombudsman