DRN-6221615

The complaint

Mr H, the director of TG Ltd, complains that Wise Payments Ltd (Wise) failed to prevent his company from falling victim to a purchase scam. The complaint has been brought to the Financial Ombudsman Service by a professional representative, J.

What happened

The background to the case is well known, so I won't repeat everything here. On 14 March 2025, Mr H opened a Wise account for TG Ltd and made a payment of £13,603.92 to an international payee. He believed he was transferring funds to a legitimate business for the purchase of supplies. Unbeknown to him at the time, he had been corresponding with a scammer who had deceived him into thinking he was a representative of that business.

The scam was reported to Wise on 19 March 2025. Mr H learned from a business associate that the supplier he thought he was dealing with had no website and the name of the individual he had been corresponding with was referenced as defrauding others in a similar way. Wise was unable to recover any of the funds from the receiving account which was held with its European subsidiary, Wise Europe SA.

After Wise rejected TG Ltd's complaint seeking reimbursement, the case was referred to our service. One of our investigators recommended that TG Ltd should be reimbursed in full and paid 8% simple interest from the date of the payment to the date of settlement. Wise disagreed with that outcome and asked for a final decision from an ombudsman.

I issued a provisional decision on this case on 25 February 2026 where I was minded to reach a different outcome to the investigator and not uphold this complaint. I said:

There's no doubt that TG Ltd was the victim of a scam and I'm sorry that the company has suffered a loss. I appreciate that my provisional findings will be very disappointing to Mr H, so I will try to carefully outline why I've reached a conclusion different to our investigator.

Initial Considerations

It is accepted that TG Ltd authorised the disputed payment. Under the Payment Services Regulations 2017, the company is presumed liable for the loss in the first instance in circumstances where a transaction is authorised. As this was an international payment, The Faster Payment Scheme (FPS) Reimbursement Rules also do not apply to this transaction either.

However, that is not the end of the matter. When taking into account the relevant regulations, industry guidance and good practice, there are circumstances in which Wise may be expected to take additional steps or carry out further checks before processing a payment, to help protect customers from the risk of fraud.

Should Wise have done more prior to processing the payment?

Wise didn't intervene with the payment that TG Ltd instructed it to make, although it asked Mr H for the purpose of the payment and provided a relevant written warning before he proceeded. Our investigator felt Wise should have carried out a human intervention by speaking to Mr H before the transaction was released. Among other things, this was because it was an international transfer of a high amount and carried a heightened risk of not being recoverable.

While I believe that Wise should have questioned the purpose of the payment and provided a tailored written warning, I disagree that this payment was sufficiently concerning that it required a human intervention from Wise. I say this because:

- *This was a business account, and although it had been opened that same day and there was no past activity to compare it to, it isn't uncommon for companies to send payments of this size in a single transaction.*
- *The fact that this was an international payment is not in itself high-risk to require human intervention. One of Wise's core services is providing accounts for making international payments at competitive rates, and—as referenced in submissions—this was the reason TG Ltd opened the account. In this context, such a transaction is not unusual.*
- *The investigator suggested that the payment was made immediately after TG Ltd had first credited its Wise account with the same amount from its NatWest account, which she considered suspicious. I don't think this reflects what happened. Rather than two separate transactions, the payment was funded through the Wise app via open banking, where TG Ltd entered its NatWest details and authorised payment directly to the intended recipient. Wise then requested the funds from NatWest, converted them to EUR, and transferred them. This all formed part of a single transaction carried out by Mr H, and I don't consider that to be unusual either.*

Despite what I've said above, I accept it is still a high value transfer to a new payee. So I think it would have been appropriate for Wise to ask TG Ltd about the purpose of the payment and provide a tailored written warning about the associated scam risks based on their answer.

As mentioned, Wise asked Mr H for the payment purpose and he selected 'paying an invoice'. The warning Wise provided to him was as follows:

- ***Do you know and trust who you're paying?***
  If you're paying upfront for goods or services, always read independent reviews first to make sure the business is trustworthy.
- ***Has someone asked you to change their regular bank details?***
  Verify the request with a person you trust first. Scammers can pretend to be people who regularly invoice you and ask you to pay a new account.

I don't consider the warning to have clearly highlighted the main scam risk associated with paying an invoice. Specifically, the possibility that correspondence can be intercepted and the invoice altered. This is a frequent feature of invoice-interception scams, where fraudsters manipulate details obtained through channels such as email.

In my view, a suitably tailored warning should have advised Mr H to independently confirm any bank details received via an invoice or written communication. This could include calling the business using a phone number obtained from a reliable external source rather than the invoice or email chain, or verifying the information in person.

<u>Would such an intervention have made a difference?</u>

This is the key question of this complaint, and having reviewed all the available evidence and information about this scam, I'm not persuaded that an intervention of the kind described above would have stopped TG Ltd from making the payment.

In my view, the scam was sophisticated and very difficult to uncover at the time Mr H was making the payment. He and J have outlined the various due-diligence checks that were carried out before making the payment. I can see that the supplier was found through reputable sources before searching for it on Google. What made things more difficult in this case to uncovering the scam is the fact that the genuine business did not have its own website. The scammer was seemingly able to exploit this by creating a convincing website in

the supplier's name and there was no clearly identifiable alternative to spot that this was illegitimate. I therefore don't criticise Mr H for making contact via that website or for being unaware of the genuine supplier's lack of an online presence, which was only later confirmed by a representative of its parent company.

I have also reviewed the correspondence with the scammer, and I consider the impersonation to have been convincing, with no clear red flags I would reasonably have expected Mr H to identify. The scammer used an email domain that appeared legitimate, and their communications were credible throughout. Once specific goods had been selected, they provided a professional-looking invoice. J also explained that the pricing was consistent with previous purchases and comparable suppliers that TG Ltd had used, which made the offer appear credible rather than "too good to be true." Mr H also said he had searched online for reviews, warnings or red flags associated with the company name and website with nothing concerning found.

In those circumstances, I can understand why Mr H believed he was dealing with a legitimate business, and I do not think he acted negligently. I therefore need to consider whether an intervention from Wise of the kind described above would, on balance, have prompted him to reflect, take further steps, and ultimately uncover the scam.

On balance, I am not persuaded that it would have in view of what I've seen. Given the extent of checks that had been carried out already, I don't think an appropriate warning would have likely triggered concern as it would have covered most things Mr H had done already. Even if he had sought to independently verify the bank details to counter a possible invoice interception risk, as an appropriate warning should have advised, I think it is highly likely this would not have succeeded in the circumstances of this case.

At the point of payment, the scammer was already in direct contact with Mr H over WhatsApp and there was no clearly identifiable alternative site to reveal the known website was illegitimate. In those circumstances, I consider it likely that Mr H would either have called the scammer directly via WhatsApp to verify the details or relied on contact details taken from the fraudulent website. Unfortunately, either route would have led to the same outcome: the scammer would simply have confirmed that the bank details on the invoice were correct.

I would also like to add that I'm not persuaded a human intervention would have uncovered the scam—even if I agreed with the investigator that one was necessary. The investigator's conclusion appeared to rest on the idea that Wise would have requested the invoice and compared it with information it held about the beneficiary account. However, for the reasons already outlined regarding the due-diligence steps taken and the scammer's correspondence, I do not think Wise would necessarily have become so concerned during questioning that it would have demanded sight of the invoice and then identified discrepancies with the receiving account. Given the due diligence Mr H had already carried out, and the fact he had been provided with a professional-looking invoice, I think he would likely have answered any routine questions in a way that would not have prompted Wise to escalate matters to that level.

I'm very sorry that TG Ltd has suffered this loss. But for the reasons above, I don't think Wise is responsible for what happened, and I can't fairly recommend that it reimburses the loss

My provisional decision

For the reasons outlined above, I am minded not to uphold this complaint.

--END--

Wise accepted my provisional decision but TG Ltd disagreed. On the company's behalf, J responded with several points, including:

- That I had applied too high a threshold by requiring "certainty" that an appropriate warning would not have prevented the loss. The correct test, J said, is whether there was a real and substantial chance that the outcome could have been different, not whether it definitely would have been.
- That I wrongly assumed the only verification routes available to Mr H were the scammer's WhatsApp number and the fraudulent website. J said alternative verification options were available which could have exposed the scam, but which had not been considered.
- That it was incorrect to rely on Mr H's diligence prior to the payment to conclude that an appropriate warning would not have made a difference. J said Mr H's earlier checks were aimed at confirming the existence and legitimacy of the supplier, not verifying the bank details provided — which a tailored warning would have prompted him to do.
- That despite saying that Wise's warning was inadequate, and that Mr H acted without negligence, I then reached a contradictory conclusion by finding that Wise bore no responsibility for the loss.
- That the beneficiary account showed a materially different name after the payment was made—one that bore no resemblance to the payee Mr H intended to pay. Wise should have flagged this discrepancy prior to payment being made.
- That the invoice contained a Belgian IBAN despite the supplier being based in the Netherlands, and that a properly tailored warning would have drawn Mr H's attention to this inconsistency and prompted him to seek verification.

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.

Having carefully considered J's response to my provisional decision, my conclusions remain unchanged and I will not be upholding this complaint.

I am very aware that I have summarised J's responses to the provisional decision in less detail than they were provided, and in my own words. No discourtesy is intended. Rather, I have focused on what I consider to be the central issues. If I have not mentioned a particular point, it is not because I have ignored it — I have not. I am satisfied that I do not need to address every individual argument in order to reach what I consider to be the fair and reasonable outcome. Our rules allow me to do this, reflecting the informal nature of our service as a free alternative to the courts.

I think it is important to address some of the conclusions J appears to have reached in response to my provisional decision. First, I did not reach a finding based on *certainty* that an intervention of the kind I considered appropriate would not have made a difference. My conclusion was, and remains, based on what I consider *likely* to have happened on the balance of probabilities in light of the available evidence.

It is also important to reiterate that the starting point is that TG Ltd is liable for a loss arising from an authorised payment. As this was an international payment, there is also no protection that guarantees reimbursement from Wise in circumstances where the company fell victim to a fraud like this, even where a scam warning may have been found to be insufficient.

Where it is concluded that a warning or intervention should have gone further, our approach is to then consider whether the additional or recommended action would have been likely to make a difference in preventing the loss. That is the crux of the matter in this case. If, on balance, I do not consider it likely that such action would have changed the outcome, then I cannot reasonably recommend that Wise reimburse the losses.

On the intervention point, I remain of the view that a tailored written warning of the kind I outlined in my provisional decision was reasonably to be expected in the context of this payment. My reasons for concluding that the circumstances did not warrant the payment being held or requiring human intervention also remain unchanged.

I do not accept the additional points put forward by J as to why the payment should have been held. It was suggested that the payee name entered by Mr H bore no resemblance to the name on the receiving account. Respectfully, that is not the case. The names were very similar — the differences were limited to the omission of the final two characters and the "Limited" suffix. I do not consider this minor discrepancy sufficient to reasonably indicate fraud or to require the payment to be flagged and held.

J also noted that the invoice presented a Dutch business while the payment was made to a Belgian bank. While that is correct, it is not clear how Wise could reasonably have identified that discrepancy at the point the payment was made. Given my conclusion that the circumstances did not warrant the payment being held or requiring human intervention, I do not consider that Wise could have been reasonably aware of this at the relevant time to highlight this to Mr H in any written warning prior to payment.

The key question is then how Mr H would likely have responded to an appropriate written warning about invoice-interception scams. At the point of payment, Mr H held no concerns about the legitimacy of the person he was dealing with, nor did he have any reason to believe the website he thought belonged to the supplier was fraudulent. I do not think it likely that a written warning in the manner I suggested would have caused him to doubt the legitimacy of the website or the individual he was corresponding with in view of the checks he'd already carried out.

I agree with J that those earlier checks were aimed at confirming the existence and legitimacy of the supplier, rather than verifying the bank details outside the invoice or email chain — which would be a key recommendation in an appropriately tailored invoice-interception warning. So, if Mr H had decided to take further action in response to such a warning, it is likely that his focus would have been on verifying the bank details he had been given.

The question, then, is how he would have sought that verification. Taking into account the position at the time of the payment, I remain of the view that Mr H would most likely have contacted the scammer directly through their established communication channel, or used the phone number or details on the supplier's website. If that had happened, then it is more likely than not that the scam wouldn't have been uncovered and the loss wouldn't have been prevented.

While I accept that the additional verification routes put forward by J were possible, and I cannot rule them out with certainty, I do not consider them as likely. This is because I do not believe an appropriate warning would have caused Mr H to question the legitimacy of the business or the individual he was dealing with to the extent that he would bypass the more straightforward and efficient option of verifying the details directly through one of the two channels I have outlined.

I am sorry that TG Ltd fell victim to this scam and lost a significant amount. But for the reasons I have outlined, my position remains the same that the losses would not have been prevented even if Wise had issued a tailored written warning of the kind I believe was appropriate. Therefore, I am unable to recommend that Wise take any further action to address the losses the company suffered.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask TG Ltd to accept or reject my decision before 10 April 2026.

James Abbott
Ombudsman