DRN-5334017

The complaint

Miss B has complained that Wise Payments Limited ("Wise") failed to protect her from falling victim to a job scam, and hasn't refunded the money she lost in the scam.

What happened

I issued a provisional decision ("PD") in January 2025 explaining why I was minded to uphold Miss B's complaint. I gave both parties the opportunity to respond to my provisional findings – Miss B accepted them but Wise didn't, and it provided further comments.

I've included an extract of my PD below, as well as Wise's response.

> **What happened**
>
> The background of this complaint is already known to both parties, so I won't repeat all of it here. But I'll summarise the key points and then focus on explaining the reason for my decision.
>
> Miss B has used a professional representative to refer her complaint to this service. For the purposes of my decision, I'll refer directly to Miss B, but I'd like to reassure Miss B and her representative that I've considered everything both parties have said.
>
> Miss B has explained that in September 2023 she was approached on a messaging app by an individual ("the scammer") claiming to work for a recruitment company, who was recruiting for a home-based role. Miss B says the contact wasn't completely unsolicited as she'd been actively seeking work and she'd applied for a number of jobs, and she says it's common for recruiters to use the messaging app that the scammer contacted her on.
>
> Miss B expressed an interest in the role and the scammer told her she'd pass Miss B's details on to a colleague, who would be in touch to explain the role in more detail. When this contact was made, the second individual (also referred to as "the scammer") explained that the role involved leaving five-star reviews on hotels in order to increase the rankings in product searches.
>
> The scammer explained Miss B would be given access to a work platform, and she'd have an account manager. She was told she'd need to complete 66 tasks in return for £40-£60 per day, plus a bonus of £380 for logging in on five consecutive days. Miss B was directed to the work platform to create an account and she's explained that it looked professional and slick, setting out the hotels and packages available, information about the company she was working for, and information about her account.
>
> The scam began when the scammer directed Miss B to create an account on the work platform via a link to what appeared to be a registration page. Miss B believed this was a genuine process so she followed the instructions and provided her identification details, which she explains is a step she recognises as a standard Know Your Customer (KYC) requirement. She says this level of security added to the illusion that she was registering for a legitimate business and felt reassured by the professional appearance of the website and the work platform.
>
> Once her account was set up, Miss B was able to see her account balance, amongst other things, which reassured her that her earnings were secure. She was also added to a

messaging group where other supposed employees claimed to be completing similar tasks, with many of them discussing successful withdrawals. Again, Miss B explains that these interactions helped reinforce the illusion of legitimacy.

On 22 September 2023 Miss B was instructed to make an initial payment of £50 to verify her account, and the scammer assured her that this amount would be included in a bonus she would receive after completing her initial tasks. Miss B made the payment from her Wise account without any additional security checks or intervention. Miss B then completed the assigned tasks and noticed her commission increasing on the platform. When she asked to withdraw her earnings, the scammer claimed that her account had a negative balance due to her exceeding her allowance. She was told she needed to clear the negative balance to upgrade her account and access higher commission.

Over the next two days Miss B made four further payments totalling £248.40 to clear the alleged negative balance. She says that despite the payments being sent to new payees, Wise failed to flag or question the transactions. On 25 September 2023, as she believed she'd resolved the issue around her negative balance, Miss B made a further five payments on instruction of the scammer. She says these transactions were also not subject to any additional checks or intervention by Wise.

The payments Miss B made as part of the scam were as follows:

	Date	Amount
1	22/09/2023	£50.00
2	23/09/2023	£48.77
3	23/09/2023	£32.20
4	24/09/2023	£44.59
5	24/09/2023	£123.75
6	25/09/2023	£50.21
7	25/09/2023	£140.17
8	25/09/2023	£514.06
9	25/09/2023	£1,348.00
10	25/09/2023	£3,351.04
	Total	**£5,700.08**

When Miss B attempted to withdraw her funds, the scammer demanded a withdrawal fee which she says was larger than the amount she'd already paid. Miss B told the scammer she couldn't pay, and she's described how at that point the scammer's tone changed and they became aggressive, and tried to pressure her to borrow money from family or friends or take out a loan. This was when Miss B realised she'd been scammed.

Miss B contacted Wise to report the scam. She described what had happened, but she says the responses she received felt automated and unhelpful. She was asked to send screenshots of her conversations with the scammer, but she says she wasn't given any help on how to protect herself from future scams. Miss B believes Wise failed to meet its responsibilities, leaving her feeling unsupported and vulnerable.

I've noted Miss B's comments that she was particularly susceptible to the scam because she lacked experience in this area and was actively seeking a job. She's added that the scammer's professionalism, constant communication, and use of platforms she perceived as credible all contributed to her trusting them. She also says the absence of effective intervention or fraud alerts from Wise allowed the scam to continue further than it should have.

Miss B made a complaint to Wise. Wise didn't uphold the complaint and in its response it said that it had shown Miss B several warnings related to job scams before she made the payments, but she chose to proceed regardless. So it didn't agree that it was liable to refund any of Miss B's losses.

Miss B remained unhappy so she referred the complaint to this service.

Our investigator considered everything and didn't think the complaint should be upheld. Although at the time the investigator issued her view Wise hadn't sent its business file, she explained that Miss B had given Wise the incorrect payment purpose for some of the payments – as she'd said she was sending some of the payments to friends and family – so she didn't hold Wise responsible for what happened.

As Miss B didn't accept the investigator's opinion, the case has been passed to me to make a decision.

What I've provisionally 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.

Since our investigator expressed her opinion on the complaint I've been in touch with Wise and I've now received its business file. And having reviewed the information within it I'm now proposing to uphold the complaint.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And in this case it's not in question whether Miss B authorised these payments from leaving her account. It's accepted by all parties that Miss B gave the instructions to Wise and Wise made the payments in line with those instructions, and in line with the terms and conditions of Miss B's account.

But that doesn't always mean that the business should follow every instruction without asking further questions or intervening to ensure requests coming from their customers are firstly genuine, and secondly won't result in harm.

At the time the scam took place Miss B hadn't used her account, so Wise didn't have any prior account activity to understand what Miss B's normal usage pattern looked like. Whilst that doesn't completely absolve it from being on the lookout for fraud or signs of financial harm to its customers, it does mean that Wise would've needed to rely on information it knew more widely about how its customers used their accounts, and what scams more broadly looked like.

Did Wise intervene, and if so, how?

Wise says that for eight of the payments Miss B made she was asked for the purpose of the payment, and presented with a list of options. Wise says Miss B selected different reasons; for payments one and two she selected she was "paying to earn money by working online" and for payments three to five, seven, nine and ten she selected "Sending money to friends and family". Wise didn't ask for the purpose of payments six or eight, or show a warning for them. It says it showed Miss B a corresponding warning for the other eight payments, based on the purpose she'd selected.

Did Wise do enough to intervene?

Wise's system triggered further questions and an intervention from the first payment Miss B made, so I've considered whether the way it intervened from that point was proportionate. And I've concluded that by asking for the payment purpose, Wise gained information that ought to have raised its suspicions that Miss B was falling victim to a scam.

Whilst the first payment was for a low value, it's very rarely legitimate for someone to pay up front to earn money. This is a well-known scam that has been prevalent for several years, and as Wise's fraud detection system triggered and asked Miss B for the payment purpose,

I'd have expected Wise to react accordingly to the information Miss B gave it in response. This would most likely either have been to check whether Miss B had answered its question about the payment purpose incorrectly, or to probe her further on why she was making the payment, with a view to giving her a better automated warning about the risks associated with task-based job scams. As an example I'd have expected this warning to include information that brought to life what was likely happening, and a clear and unambiguous warning that this was likely a scam.

Wise has provided a copy of the warning it says it showed for the first payment. The warning is generic in nature with no specific warning to any particular type of scam, and includes the text "So, while your answers don't suggest this is a common scam, talk to someone you trust first. A second opinion can help you send safely".

Having considered this, Wise failed to proportionately intervene from the first payment Miss B made. Given the date the payment was made – in late 2023 – I'd have expected Wise to go some way to protect Miss B from foreseeable harm, and to use the information it had been given in order to do that. But by giving Miss B a warning saying her answers suggested she *wasn't* being scammed, it failed to take the opportunity to uncover the scam at that point and prevent Miss B from losing the money that she did.

Is Miss B responsible for any of her losses?

In considering the allegations against Wise it's also necessarily to consider whether Miss B played any part in falling victim to the scam. That's to say whether Miss B acted ignored or bypassed warning signs to a point that could be considered negligent.

I accept that Miss B has fallen victim to a carefully crafted scam here, and whilst I haven't seen the work platform Miss B used, I've seen previous examples of them and I know they can be very convincing.

But it's very unusual for a recruiter to contact a prospective candidate and offer them a job through a messaging app, without having ever spoken to them. I'm also not aware that Miss B received any kind of paperwork or employment contract showing what she thought she'd been offered, or what she'd agreed to do. This, as well as having to pay to earn money in return, isn't a plausible scenario.

With this in mind I think it's fair for the responsibility of Miss B's loss to be shared equally between Miss B and Wise.

In response to my PD Wise made the following points:

- Miss B only selected the option "paying to earn money by working online" for the first two payments – which were for relatively low values.
- These initial payments didn't create enough suspicion to justify intervention, as otherwise Wise would need to block all payments where this purpose is given.
- It's unclear why Miss B changed the payments purpose to "sending money to friends and family" for the remainder of the payments, especially as she knew the option to select "paying to earn money by working online" was available.
- The warnings for the first two payments could've been stronger, but Miss B deliberately misled Wise by giving incorrect information about the reasons for payments 3 – 10. So no level of intervention would've prevented the scam.

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 thought carefully about Wise's points, I'm still upholding the complaint. I'll address each point in turn.

Miss B only selected the option "paying to earn money by working online" for two payments

Whilst I accept that Miss B only selected the correct payment purpose for the first two payments, and that these payments were of low value, this doesn't diminish the significance of Wise's intervention at that stage. The purpose of Wise's fraud detection system is to identify and mitigate the risk of fraud early. By asking Miss B for the payment purpose, Wise obtained information that should've triggered further action. The fact that the payments were low in value doesn't negate Wise's obligation to assess the broader context and potential risk of harm, particularly given the well-documented nature of task-based job scams. Whilst I don't know for certain what would've happened, early intervention at this stage could've prevented Miss B from making the further, larger payments.

The level of concern created by said payments

My decision doesn't suggest that Wise should automatically block all payments where the purpose "paying to earn money by working online" is given. Instead, it highlights that Wise already had a system in place to flag and review such payments. Given that Wise chose to intervene by asking Miss B about the payment purpose, it's reasonable to expect that it would then properly assess the information Miss B gave in response. The information provided by Miss B – that she was paying to earn money online – was a known scam indicator. Wise had an opportunity to engage more meaningfully at this stage, which could've included tailored warnings or additional queries to better understand Miss B's circumstances and alert her to the risks involved. So my view remains that Wise's intervention was inadequate.

The reason for Miss B changing the payment purpose

Whilst it's unclear why Miss B changed the selected payment purpose for subsequent transactions after the second payment, this doesn't absolve Wise of responsibility for the inadequate intervention at the outset. Had Wise provided clearer and more targeted warnings for the first two payments, Miss B may have been deterred from proceeding with further payments, regardless of the stated purpose. Scammers often manipulate victims into misrepresenting payment purposes, particularly when they realise that financial institutions are flagging transactions. This makes early intervention even more critical; if Wise had taken appropriate steps in response to the first two payments, Miss B may not have proceeded with the scam payments at all.

Miss B deliberately misleading Wise

I acknowledge that Miss B later changed the payment purpose and told Wise she was paying a friend or family member. But in this case, the responsibility was with Wise to provide clear and effective warnings at an early stage. The initial warnings given were generic and didn't adequately address the specific risks of task-based job scams. Had Wise provided a stronger, more tailored warning at the outset, Miss B might not have fallen "under the spell" of the scammer and may have reconsidered her actions before making further payments. The fact that she later changed the payment purpose, possibly as a result of being coached by the scammer, doesn't eliminate Wise's duty to have taken reasonable steps to prevent foreseeable harm when it first identified the potential risk.

Having reviewed everything again, including Wise's response, I don't consider that it provides sufficient grounds to change my decision. Wise had an opportunity to intervene effectively when it first flagged Miss B's payments, but the actions it took weren't proportionate to the known risks associated with the type of scam in question. A more tailored and effective warning at the outset could have prevented Miss B's subsequent losses, so my decision to uphold the complaint remains unchanged.

Putting things right

To put Miss B back in the position she'd have been in had Wise done what it should've, Wise needs to:

- Refund 50% of the losses Miss B experienced from the first payment, and;
- Pay 8% simple interest on each amount, from the date each payment left Miss B's account until the date of settlement*.

*If Wise considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Miss B how much it's taken off. It should also give Miss B a tax deduction certificate if she asks for one.

My final decision

I uphold Miss B's complaint against Wise Payments Limited and I require it to put things right as I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss B to accept or reject my decision before 17 March 2025.

Sam Wade
Ombudsman