DRN-4291809

The complaint

Mr M complains that Wise Payments Limited won't refund money he lost when he was the victim of a scam.

Mr M is represented by a firm that I'll refer to as 'R'.

What happened

The background to this complaint is well known to both parties and so I'll only refer to some key events here.

In March 2023 Mr M was the victim of a task-based job scam after being contacted on a mobile messaging service app. He was told by the scammer he could earn daily commission of up to $1,000 from completing tasks that involved simulating the purchasing of items – as this would boost the marketability of products for big brands. Mr M says he reviewed the firm's website, which appeared very professional, and thought he was working for a legitimate company (whose website address was similar the scam firms). And, through an internet search, he didn't find any negative reviews but confirmed the location of the firm's headquarters.

The scam required Mr M to purchase and send crypto to the scam platform – which was used to simulate the purchase, thereby completing the task and adding commission to Mr M's account. Mr M realised he'd been scammed when he was unable to fund the account and was told by the customer service function his account would be frozen and that he'd be unable to withdraw his funds.

Mr M made the following transfers, to a number of different payees, to purchase crypto as part of the scam:

Date (time)	Payee	Amount
14 March 2023	A	£33
16 March 2023	B	£11
20 March 2023	C	£250
20 March 2023	D	£140
20 March 2023	E	£250
21 March 2023	F	£400
21 March 2023	G	£25
21 March 2023	H	£3,600
21 March 2023	H	£3,000*
21 March 2023	H	£3,600*
22 March 2023	I	£5,000*
22 March 2023	I	£4,000*
22 March 2023	I	£1,800
22 March 2023	I	£5,000
22 March 2023	I	£4,000*
22 March 2023	I	£4,000*

24 March 2023	J	£10,000
24 March 2023	K	£10,000
24 March 2023	L	£3,000*
24 March 2023	M	£3,500
24 March 2023	N	£1,500*
24 March 2023	N	£5,000*
24 March 2023	0	£3,100*
	Total:	£71,209

*Wise provided an online warning for these payments

There was also another payment of £3,500 attempted on 24 March 2023 but this was returned.

R complained to Wise, on Mr M's behalf, in April 2023 about what happened. They said Wise failed to protect Mr M from the scam by not identifying the above payments as out of character and indicative of fraud. And they considered the fraud could've been prevented had Wise appropriately intervened before processing the payments – as questioning Mr M about the purpose of the payments would've uncovered that he was making payments to purchase crypto as part of a job opportunity, which is a type of scam known to Wise and that has been on the rise due to the cost-of-living crisis. And so, Wise ought to have told Mr M about how these scams work and stopped him making any further payments. R wanted Wise to reimburse Mr M for the loss he suffered and to pay 8% interest.

Wise rejected the complaint. In short, they said:

- Once a transfer is sent out to the recipient's bank, the funds are no longer under Wise's control. And the obligation of ensuring the legitimacy of the recipient on any given transaction lies with the sender of the payment.
- Wise doesn't have the ability to be involved in disputes between the sender and recipients. They recommend to all customers to perform their investigations on that person before setting up a payment – which is expressed across various parts of their system, including their FAQ page (which incorporates part of the Customer Agreement that Mr M agreed to when setting up his Wise account).
- 21.1 of their Customer Agreement says:

> **We are responsible to you for foreseeable loss and damage caused by us**…We are not responsible for any loss or damage that is not foreseeable. Loss or damage is foreseeable if either it is obvious that it will happen or if, at the time contract was made, both we and you knew it might happen, for example, if you discussed it with us during your account sign up process.

  As stated, they cannot be made liable for any circumstances beyond their control – such as when a loss occurs as a result of fraudulent behaviour on behalf of the recipient after a payment has been made to them.
- They can only control and monitor activities in relation to their own customers and while a transaction is pending in their system. And once they were made aware of the recipient bank account possibly being used for scam purposes, they took appropriate action to prevent further transfers being made to them through their service.
- They were unable to recover any of the funds transferred because the recipients had already moved the funds.
- They completed the transfers as directed by Mr M and fulfilled their contractual obligations by doing so.

The complaint was referred to the Financial Ombudsman and our Investigator thought it should be upheld in part. She noted that Wise provided Mr M with online warnings on ten of the payments he made as part of the scam – which were generated by him selecting 'Paying to earn money by working online' as the payment purpose. But she thought Wise ought to have contacted Mr M at the point of the third payment to payee H on 21 March 2023, as he'd sent over £10,000 in a single day for a high-risk payment purpose.
Had this happened, our Investigator thought Wise could've prevented Mr M's loss from this point onwards. But she also thought Mr M should take some responsibility for his loss too – as the online warnings should've given him reason for concern, thereby prompting him to carry out further checks before proceeding. And noted that there is a lot information online about working from home scams that Mr M could've easily accessed. So, she thought Wise should refund 50% of the payments – totalling £31,750. But she didn't think any additional interest, for loss of use of money, should be added as Mr M borrowed the money lost to the scam from friends.

R accepted our Investigator's recommendation. Wise did not and, in short, said:

- It's not reasonable to expect Wise to suspend and directly contact customers any time a payment could be considered high risk – especially where they have already provided online warnings and the customer has chosen to continue sending money.
- Wise is primarily a money remittance service and not a bank. And Mr M's account activity relating to the scam was in keeping with how their product is designed and how customers use their platform.
- While this may be a typical hallmark of fraud or cause for concern for a bank, this activity isn't considered suspicious to Wise – and, in fact, is one of the unique aspects of their financial product which is marketed as being quick and easy. It's therefore not feasible for them to suspend and question a customer for every transfer that could be considered high risk by a bank.
- Their scam warnings should've been sufficient as they clearly set out the type of scam Mr M was falling victim to. And, as the Investigator explained, Mr M should've carried out more due diligence and research – especially after the first online warning.
- Wise took reasonable action to warn Mr M about the scam but he chose to ignore this on ten occasions. And so, he should be held responsible for his entire loss.

The matter was referred 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.

Having done so, I've come to same overall conclusions as our Investigator and for similar reasons. I'll explain why.

In broad terms, the starting position in law is that an electronic money institute (EMI) – like Wise - is expected to process payments their customer authorises them to make. Here, it isn't disputed that Mr M knowingly made the payments to the scammer. I appreciate Mr B was tricked by the scammer into thinking he was making the payments as part of a genuine job opportunity. Nevertheless, I'm satisfied the payments were authorised by Mr M. So, under the Payment Services Regulations 2017 and the terms of his account, Wise are expected to process the payments and Mr M is presumed liable for the loss in the first instance.

Wise is an EMI and so, as they've pointed out, Mr M's account with them isn't a bank account. This means it isn't subject to the same fraud prevention expectations set out in guidance and regulation that a current account with UK bank provider otherwise would be. That said, it doesn't mean Wise has no obligation to Mr M. I'm satisfied Wise, under PRIN 2.1 in the Financial Conduct Authority's handbook, has a duty of care to treat their customers fairly. And Wise is also expected to be on the lookout of financial crime – and their terms and conditions reflect that they will take action if they suspect fraudulent activity. From this, I'm satisfied Wise should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had systems in place to look out for unusual transactions or other signs that might indicate that their customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which financial institutions are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

I therefore need to decide whether Wise acted appropriately when handling Mr M's payments – specifically, whether they should've done more before processing them and, if they had, would it have made a difference. And so, I've firstly looked at whether the instructions given by Mr M to Wise were unusual enough - in relation to his typical account activity – to have expected Wise to have identified Mr M was at risk of financial harm from fraud.

When considering this, I've kept in mind that EMIs process high volumes of transactions each day – with 'quick and easy', as Wise have point out, a feature offered by them to their customers. Because of this, there is understandably a balance for Wise to find between allowing customers to be able to use their account and questioning transactions to confirm they're legitimate. I therefore wouldn't expect Wise to suspend and question every transfer made by a customer, but only those whereby there are reasonable grounds for them to suspect there is risk of financial harm from fraud.

Having looked at Mr M's account usage for the twelve months prior to the scam occurring, it was typically used for low value day to day transactions with occasional payments of a higher value – such as payments to an estate agent for £1,650, and another single payment in September 2022 for £5,000. I therefore don't think the payments – up until the first made to payee H – would've stood out as unusual or out of character to Wise.

On the second payment to payee H, Wise did however ask Mr M to select the reason for the transfer – and he selected 'Paying to earn money by working online'. This then prompted the following online warning:

> *"**Have you been asked to pay to earn money?***
>
> *Stop – this is a scam. Scammers will ask you to pay, and then start earning money by watching ads or writing reviews.*
>
> ***Have you already been paid a small amount?***

Scammers might pay you a small amount first to gain your trust. Then, they'll ask you to pay them to earn larger amounts."

Mr M proceeded to continue with making this payment.

I think this warning was both clear and relevant to Mr M's circumstances, as well as sufficiently tailored to the payment purpose he disclosed. I therefore think Wise acted appropriately by providing this warning at this point. And so, I wouldn't have expected Wise to have taken any additional steps before processing this payment.

Mr M then made a third payment to payee H, on the same day, and gave the same reason for the transfer – thereby prompting Wise to provide Mr M with the above online warning again. Having carefully thought about this, I think at this point it would've been reasonable for Wise to have carried out additional checks – beyond providing the online warning – before processing this payment. This is because Mr M made five payments to three different new payees on the same day – with the last three payments, sent to the payee H, totalling over £10,000. This was an unusual pattern of spending and out of character for Mr M based on his typical account usage. And given Mr M had disclosed to Wise on two of the payments that the reason for transferring the funds was 'Paying to earn money by working online', I think Wise had sufficient reason to suspect Mr M was at significant risk of financial harm from fraud – especially as Wise explain in their online warning that this type of payment reason, whereby someone is asked to pay to earn money, is a scam. So, I think it would've been reasonable for Wise to have contacted Mr M to discuss the third payment to payee H before processing it.

I've gone onto think about, had Wise done so, what would've likely happened. And as Mr M was honest when providing the purpose of the payments online, I've no reason to think he wouldn't similarly have been honest in discussing the payments with Wise. I therefore think, upon appropriate questioning, Mr M would've likely explained he was purchasing crypto as part of a job opportunity whereby he completed tasks that involved simulating the purchasing of items. Given Wise's awareness of the prevalence of task-based job scams, they would've known – as per their online warning – that this was scam.

It follows that I think Wise ought to have told Mr M that he was being scammed and advised him not to proceed with making any further payments. When considering whether Mr M would've been receptive to such advice I've taken into consideration that, even though Wise provided what I considered to be a clear and relevant online warning on ten occasions, he continued to make the payments to the scammer. But while I think Mr M may not have acted reasonably by ignoring these warnings, which I'll go on later to explain, I think a conversation that included Wise providing a tailored warning as well as a recommendation not to proceed with the payment(s) would've been more impactful – and that it would've resonated with Mr M more so than a written online warning. It would've also provided Wise with the opportunity to direct Mr M to information online, which was easily accessible, about task-based job scams. And I consider this would've likely been enough to break the spell Mr M was under from the scammer and made him realise the job opportunity wasn't legitimate. So, on balance, I think it's more likely Mr M wouldn't have proceeded to make the payment(s) if Wise had contacted him before processing it.

But even if I were to think Mr M may not have been receptive to such a warning, I've also considered term 25.3 of Wise' Customer Agreement, which says:

*"**We may suspend your Wise Account for security reasons.** We may suspend your Wise Account or restrict its functionality if we have reasonable concerns about:*

(a) the security of your Wise Account; or

(b) suspected unauthorised or fraudulent use of your Wise Account"

Given I'm satisfied Wise would've known that Mr M was falling victim to a scam, I think it would've been reasonable for Wise to have stopped the payment(s) from being made – as their terms allow – given Mr M's account was being used for fraudulent purposes (albeit he was the victim). I therefore think, for the reasons I've explained, Wise could've prevented Mr M's loss from the point of the third payment to payee H onwards.

I've also thought about whether Mr M did enough to protect himself from the scam and I don't think he did. Although I appreciate Mr M believed the job opportunity was genuine, I think he ought reasonably to have had concerns about its legitimacy and shown greater caution before making the payments. This is because Mr M was contacted about the opportunity on a mobile messaging service app, which is unusual, and the concept of simulating the purchasing of items to falsely boost their marketability doesn't sound genuine. He also made deposits for significant amounts of money without receiving any of the expected returns. Furthermore, while I think Wise didn't do enough to protect Mr M from the scam, he was nevertheless given multiple written warnings and he made the payments despite that. I think it would've been reasonable to have expected Mr M to have carried out additional checks – such as researching these types of jobs/scams online – before making the payments, which he didn't do.

Wise argue that Mr M acted unreasonably by choosing to ignore these warnings and so he should be held responsible for his entire loss. I've thought about this but I don't think that would be fair here. This is because, while I accept Mr M didn't do enough to protect himself from the scam, as I've explained, I likewise think Wise ought reasonably to have done more to prevent his losses too. I therefore think both parties are equally responsible for the loss Mr M suffered from the point of the third payment to payee H. And so, I think it would be fair and reasonable to make a 50% reduction in the award I'm directing Wise to pay to take account of Mr M's contributary negligence in the circumstances of this complaint.

I've also considered whether there should be any additional interest awarded. Mr M has however confirmed that he borrowed money from his friends – which will have to be repaid. So, in these specific circumstances, as Mr M didn't use his own funds I don't think it would fair to award any additional interest. It follows that I think Wise refunding £31,750 reaches a fair outcome here.

My final decision

My final decision is that I uphold this complaint in part. I direct Wise Payments Limited to refund Mr M £31,750.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 14 February 2024.

Daniel O'Dell
Ombudsman