DRN-4556328

The complaint

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

Mr V 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 April 2023 Mr V fell victim to a task-based job scam. He's explained that, at a time when he was looking for a part-time job, he was contacted by a scam recruiter on an instant messenger app offering him an opportunity with a company I'll refer to as 'A'. The scammer claimed to work for a legitimate recruitment agency.

The job involved simulating the purchase of items – as this would improve the merchant's ability to sell the items as their 'algorithm' for the products would be improved (app optimisation). To do this, Mr V was required to deposit funds onto A's platform that would be used to simulate the purchases. Mr V would then later be able to withdraw these funds along with the commission he'd earnt.

Mr V says he carried out online checks on A before he started the job, but he found no negative reviews. And information he did find appeared to suggest A were a legitimate company that described themselves as a 'digital product and services studio' - which matched the tasks Mr V believed he was completing. Because of this, and the scam platform appearing highly professional to Mr V, he went on to make the following payments to the scam via two legitimate crypto exchanges (which I'll refer to here as 'B' and 'K'):

Date	Type	Payee	Amount
8 April 2023	Debit card payment	'B'	£100
8 April 2023	Debit card payment	'B'	£120
11 April 2023	Debit card payment	'B'	£500
11 April 2023	Debit card payment	'B'	£500
11 April 2023	Debit card payment	'B'	£441.43
11 April 2023	Debit card payment	'B'	£131.15
11 April 2023	Debit card payment	'B'	£500
11 April 2023	Debit card payment	'K'	£4,000

11 April 2023	Debit card payment	'K'	£3,927.42
12 April 2023	Debit card payment	'K'	£1,372.58
		Total	£11,592.58

Mr V says he became aware he'd been scammed when he attempted to withdraw his funds, as he was told someone else was trying to claim the funds and he needed to pay 50% of his current balance.

R complained, on Mr V's behalf, to Wise on 14 September 2023 saying the payments were made as part of a scam. In short, they said:

- Wise failed to identify out of character payments that were indicative of fraud. And had Wise intervened appropriately, the fraud would've been prevented. As such, Mr V suffered a preventable financial loss which should be reimbursed.
- The scam was very convincing to Mr V. He'd been actively looking for a job and was contacted by a recruiter who appeared to be from a legitimate recruitment agency. He was added to a group chat with other freelancers who regularly posted about their success. And A appears to have been impersonating a legitimate company, with Mr V able to speak to their 'customer service' department to discuss the tasks.
- Wise, as the fraud experts, would've uncovered the scam through robust questioning. If they'd asked Mr V what he was sending the money for then he would've admitted that he was sending money for a job that he was earning commission on. Knowing these types of task-based scams are very common would've led to further questioning – that, in turn, would've resulted in Mr V explaining he'd been contacted on an instant messenger app and was being asked to top up his account to earn commission. This would've highlighted typical red flags for this type of scam and Wise could've warned Mr V.
- Wise should refund Mr V and pay 8% simple interest.

Wise didn't uphold the complaint. In short, they said:

- When a card payment is initiated by a customer, they have the option to process or cancel it within five seconds. This means there isn't an option to suspend payments and seek additional information.
- The obligation of ensuring the legitimacy of the recipient lies with the sender of the payment. Consequently, they recommend their customers perform their own investigations before setting up a payment. This fact is expressed in various parts of their system – with them referring to their FAQ page and 'Wise Card Supplement to the Customer Agreement' document.
- Wise 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.
- If they had the ability to freeze any of the card payments, Mr V would've likely continued to make them as he would've explained they were for legitimate purposes (given the due diligence he undertook).
- It is very common for Wise to be used to make card transactions to B. This is because most UK banks do not allow transactions to this platform. Wise allows card payments to crypto currency platforms regulated in the UK and EU – including to B, which is regulated in the EU.
- It is clear that another bank is Mr V's main banking platform. And it's therefore reasonable to expect that bank would have a clear understanding of Mr V's finances

and what would be considered usual activity. Each scam transaction was prefaced by adding funds to the Wise account from that bank. If this bank didn't determine these amounts as irregular to Mr V's spending habits, then it's not reasonable to expect the liability to fall to Wise.
- Wise completed the transfer orders as directed and therefore fulfilled their contractual obligations.

The complaint was referred to the Financial Ombudsman and our Investigator thought it should be upheld in part. He thought Wise ought to have had concerns that Mr V might be at risk of financial harm at the point of the £4,000 payment. And had Mr V been questioned about the payment, he would've likely explained to Wise that he was making it as part of a task-based job. Our Investigator thought this should've put Wise on alert that Mr V was likely the victim of a scam and, accordingly, a meaningful warning should've been given – which would've prevented Mr V's losses from that point.

Our Investigator thought Mr V should share responsibility for his loss. And so, he recommended Wise refund 50% of the last three payments – along with paying 8% simple interest for loss of use of money. He also didn't think Wise could've done anything to recover Mr V's money – as chargebacks would likely have been unsuccessful, given he received the service from the crypto exchanges.

Wise didn't agree and, in short, they added:

- They don't agree that Mr V making repeated payments to the same merchant, as part of the scam, was unusual activity for him. This is because his recent prior account usage showed he'd made multiple sequential payments to a merchant of over £7,000. Therefore, making payments in a short period to platforms like B or K didn't deviate from Mr V's normal account usage. Nor does the amount stand out as unusual, as Mr V had made a similar number of split transactions to a single merchant a week before the fraudulent activity.
- Since they're not Mr V's primary financial provider, they don't have access to his income or savings information. Their reference point is the use of his Wise account, and in this context, the transactions were within the previously established usage pattern.
- Many Wise customers use their Wise cards for transactions like these – especially since several UK banks have prohibited such payments. Consequently, many customers open their Wise accounts for this specific purpose. This circumstance shouldn't have triggered any red flags.
- All card payments were explicitly authorised by Mr V and they didn't exceed his established spending pattern – and no red flags were evident.
- They lack evidence indicating any additional interventions could've influenced Mr V's decision to complete the payments. Given the deceptive nature of the job scam, Mr V believed the transactions were legitimate and would likely have proceeded with them.
- As highlighted by the Investigator, there were several factors that should've alerted Mr V to suspicions around the legitimacy of the job opportunity, and he should've taken more reasonable precautions before moving substantial funds into a crypto exchange. Mr V had already therefore demonstrated a tendency to ignore red flags during the scam – and they do not consider it reasonable to expect Wise to mark these transactions with a well-established merchant as potentially fraudulent.
- Conducting verification for each transaction and recipient created on their platform would render their service impractical.

Our Investigator considered what Wise said but his view didn't change. He thought Wise should've at least provided Mr V with a meaningful tailored warning in relation to the risks

associated with payments linked to crypto – and particularly in relation to the £4,000 payment.

The matter has been passed to me to decide. I sent my provisional decision on this complaint on 12 November 2024. I said:

> *"I'm sorry Mr V has been the victim of a scam. I realise he has lost a significant amount of money, and I don't underestimate the impact this has had on him. But while I'm sympathetic to Mr V's situation, I must consider whether Wise is responsible for the loss he has suffered. And while I know this won't be the outcome Mr V is hoping for, I don't think they are. I therefore don't think Wise has acted unfairly by not refunding the payments. I'll explain why.*
>
> *In broad terms, the starting position in law is that an electronic money institution (EMI) is expected to process payments that their customer authorises them to make. It isn't disputed that Mr V knowingly made the payments from his account – albeit under the direction of the scammer – and so, I'm satisfied he authorised them. Therefore, under the Payment Services Regulations 2017 and the terms of his account, Wise are expected to process Mr V's payments and he is presumed liable for the loss in the first instance.*
>
> *However, taking into account the regulatory rules and guidance, relevant codes of practice and good industry practice, there are circumstances where it might be appropriate for Wise to take additional steps or make additional checks before processing a payment to help protect customers from the possibility of financial harm from fraud.*
>
> *So, the starting point here is whether the instructions given by Mr V to Wise were unusual enough - in relation to his typical account activity – to have expected Wise to have identified Mr V 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. And that there is a balance for Wise to find between allowing customers to be able to use their account and questioning transactions to confirm they're legitimate. Here, the payments were made to legitimate crypto exchanges – which carries a known fraud risk as crypto scams like this have unfortunately become more prevalent. That said, many individuals do invest in crypto legitimately. And so, I wouldn't have expected Wise to have taken any additional steps before processing the first seven payments – as they were of a low value and, as Wise has pointed out, it wasn't unusual for Mr V to make multiple payments to the same merchant in a short period of time.*
>
> *I do however think the £4,000 debit card payment, and the £3,927.42 payment that followed, posed a greater risk than those that preceded it. This is because of the associated risks with crypto related transactions (including multi-stage fraud), that are well known to Wise, and the increased value of the payments. And so, I think it would've been reasonable for Wise to have taken additional steps before processing these payments.*
>
> *I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine. I've given due consideration to Wise's duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.*

Taking that into account, I think Wise ought, when Mr V attempted to make the £4,000 and £3,927.42 payments, knowing (or strongly suspecting) that the payments were going to a crypto exchange, to have provided a tailored warning that was specifically about the risk of crypto scams. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of crypto scams, without significantly losing impact.

So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common crypto scam – which, at that time, was crypto investment scams. This would've been an effective way for Wise to limit the harm caused by crypto transactions to their customers. And the warning Wise ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common crypto investment scams, for example referring to: an advertisement on social media, promoted by a celebrity or public figure; an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software and a small initial deposit which quickly increases in value.

I've thought carefully about whether such a warning would've resonated with Mr V, and to the extent whereby he wouldn't have proceeded with making the payments. Having done so, I don't think it would. This is because the most common features of crypto investment scams – which, as per above, I would've expected Wise to have highlighted – wouldn't have been relevant to Mr V's circumstances. Mr V wasn't making the payments for investment purposes, nor did he come across the opportunity through an advertisement on social media. And while there was a third party that had guided him on how to complete the tasks as part of the job, they weren't acting on his behalf.

It follows that, while I think Wise ought to have taken additional steps before processing these transactions, I'm not persuaded that even if Wise had provided a tailored written crypto scam warning that it would've deterred Mr V from making the payments. Because of this, I don't think Wise's failure to provide such a warning(s) led to Mr V suffering his loss

I've considered whether, on being alerted to the scam, Wise could reasonably have done anything to recover Mr V's losses, but I don't think they could. The only possible option for recovery here, given the payments were made by debit card, would have been for Wise to have attempted a chargeback against the payee – that being the crypto exchanges. But I don't there would've been any prospect of success given there's no dispute that the crypto exchanges provided crypto to Mr V, which he – unfortunately - subsequently sent to the fraudsters.

I have a great deal of sympathy for Mr V and the loss he's suffered. But it would only be fair for me to direct Wise to refund his loss if I thought they were responsible – and I'm not currently persuaded this was the case.

My provisional decision

My provisional decision is that I do not uphold this complaint."

R didn't agree and, in short, they provided the following points for my consideration:

- The final three payments were made to K, who had been added to the International Organization of Securities Commissions (IOSCO) register in July 2022 – and then added a further four times by different regulators before Mr V made his payments.

- They've seen the Financial Ombudsman, on other cases, say that a bank should stop and question payments to K when they were sent one month after the firm was added to the IOSCO register. This same standard should apply to Mr V's case.
- Irrespective of the fact these three payments were going to K, the Ombudsman has agreed that they were concerning enough to warrant a tailored written warning. The Ombudsman however doesn't think this would've made a difference as the warning would've been specifically tailored to crypto investment scams opposed to job/task-based scams. But job/task-based scams have been the second most prevalent scam type within the fraud landscape for some time now and so, they don't think it is reasonable to absolve an EMI of liability on the basis that crypto investment scams are slightly more common.
- This stance also directly contradicts the approach of other Ombudsmen at the Financial Ombudsman who take the view that banks and EMIs were expected to be on alert for job/task-based scams and actively taking measures to detect and warn about them (quite some time before July 2023). And they referenced various final decisions made by Ombudsmen that they consider supports their position on this – and which they believe represents the wider view of the Financial Ombudsman regarding this type of scam.
- The standard the Ombudsman is applying here is one that leaves a gaping hole in the protection of fraud victims and, in effect, means that victims of job scams will not be protected from this type of fraud simply because of overshadowing by crypto investment scams.
- It is common industry knowledge that EMIs, like Wise, are used by fraudsters to facilitate job/task-based scams due to their lack of stringent fraud controls and weak transaction monitoring. And this exact pattern of fraud is now the number one fraud trend that has been targeted at EMIs since 2018.
- The Financial Ombudsman has highlighted numerous times that banks and EMIs are expected to react to new fraud trends and job/task-based scams involving crypto have been rising for some time now – as per the final decisions they referenced.
- They therefore think an intervention should've taken place, and it follows that the scam would've been exposed had Mr V been warned of the red flags – as he would've been able to match the signs with his own circumstances.

Wise didn't respond to the provisional decision.

Now that both parties have had an opportunity to respond, I can proceed to making my final decision on Mr V's complaint.

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 thought carefully about the arguments put forward by R but, while I'm sympathetic to Mr V's situation and the loss he's suffered, I remain of the view that Wise isn't responsible for it. I'll explain why.

R has pointed out that there were active warnings added to the IOSCO register about K prior to Mr V making the payments. But I don't think Wise ought to have been on notice he was at risk of financial harm from fraud because of these warnings alone. This is because the IOSCO warnings signpost to different jurisdictions that subsequently warned that K wasn't authorised to provide certain financial services in various territories. Having considered the content of the wording, I'm not persuaded that it would be fair to expect Wise to have treated every payment to K as suspicious or high risk. This is a well-known genuine crypto platform, and most crypto-related activities are unregulated in the UK, so I don't think Wise needed to

provide a warning to Mr V about K. I note there's no suggestion that the crypto platform was involved in the scam.

I haven't received any further points in respect of whether Wise ought to have taken additional steps before processing any of the transactions prior to the payment of £4,000 to K. So, in the absence of this, I see no reason to depart from this position. It therefore follows that I consider it would've only been reasonable to have expected Wise to have taken additional steps before processing the payments of £4,000 and £3,927.42. And that a proportionate action, in these specific circumstances, would've been for Wise to have provided a written warning tailored to crypto investment scams – covering off their key features.

R argues that this approach contradicts what other Ombudsmen have determined on cases they consider similar to this one. Because of this, R feels the standard I am applying means that victims of job/task-based scams won't be protected from this type of fraud. And they consider that this type of scam has been on the rise for some time now – including before when Mr V made his payments.

I'd like to assure R that I've considered the final decisions they've referenced when deciding what I think is a fair and reasonable outcome to Mr V's complaint. While I won't be commenting on them in detail here, as I'm deciding this complaint on its individual circumstances, I think it's worth noting that the decisions R has referenced are somewhat different to Mr V's situation. Primarily, what type of intervention was warranted based on the risk identifiable to the bank/EMI at the time of the payment(s).

In the decisions R has referenced, the Ombudsmen determined the job/task-based scams could've been uncovered by the firm by way of a conversation with their customer. But here, Mr V didn't speak with Wise before processing the payments, nor, as I've explained, do I consider the payments required such an intervention – as I don't consider the payments were so unusual or suspicious whereby Wise would've had sufficient reason to suspect Mr V was at significant risk of financial harm from fraud.

At this point, I think it's worth noting that it's not possible for an EMI, such as Wise, to prevent all fraud – as it wouldn't be practical for them to question every transaction their customers make. Instead, it's reasonable for them to take a targeted approach based on the identifiable risks associated with a payment(s) - which includes reacting to new and known fraud trends. And while job/task-based scams involving crypto have sadly been on the rise, at the time of these payments, they weren't as prolific as crypto investment scams. And it would be difficult for a tailored warning to cover off every permutation and variation without significantly losing its impact.

I appreciate this means that some customers may be exposed to a greater risk of falling victim to a scam. But I think, in April 2023, a warning covering the key features of crypto investments would've been an effective and proportionate way for Wise to limit the harm caused by crypto transactions to their customers in this situation.

Unfortunately, for the reasons I explained in my provisional decision, I'm not persuaded that such a warning would've resonated with Mr V – as the common features of crypto investment scams wouldn't have been relevant to his situation. Because of this, I don't think it would've deterred him from proceeding to make the payments. And it follows that I don't think Wise's failure to provide such a warning(s) led to Mr V suffering his loss

I realise Mr V will be disappointed by this but, for the above reasons and those I set out in my provisional decision, I don't think Wise is required to reimburse Mr V's loss.

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 Mr V to accept or reject my decision before 2 January 2025.

Daniel O'Dell
Ombudsman