DRN-5652962

The complaint

Mr A complains that Wise Payments Limited (Wise) failed to protect him from losing money in a scam.

A professional representative, C, has brought the complaint to the Financial Ombudsman Service on Mr A's behalf.

What happened

The background to this complaint is well known to both parties, so I won't repeat everything here. To summarise, Mr A fell victim to a job scam after being contacted by fraudsters over Telegram. As part of this, he attempted multiple payments to a cryptocurrency platform using his Wise debit card:

Payment number	Date and time	Payee	Amount	Outcome
1	11 January 25, 9.42am	Crypto.com	£25.82	Processed
2	11 January 25, 12.09pm	Crypto.com	£1.72	Processed
3	11 January 25, 1.03pm	Crypto.com	£60.26	Processed
4	11 January 25, 2.57pm	Crypto.com	£178.64	Processed
5	11 January 25, 3.01pm	Crypto.com	£49.06	Processed
6	11 January 25, 3.46pm	Crypto.com	£1107.96	Processed
7	11 January 25, 4.20pm	Crypto.com	£3198.12	Processed
8	11 January 25, 5.01pm	Crypto.com	£7747.51	Cancelled by Wise
9	11 January 25, 5.01pm	Crypto.com	£7747.51	Cancelled by Wise

The successful payments were first credited to Mr A's Crypto.com account. To complete various tasks during the job scam, he was then instructed to purchase cryptocurrency and transfer it to a wallet that fraudsters controlled on several occasions. This ultimately led to all these funds being lost, totalling £4621.58.

Two payments attempted at 5.01pm were automatically declined and cancelled by Wise's systems after they were flagged as potentially fraudulent. At 5.24pm, Mr A contacted Wise to report that he had been scammed and asked for the processed payments to be cancelled. Wise explained this was not possible and said it couldn't recover the funds.

In March 2025, C submitted a complaint to Wise on Mr A's behalf. In summary, they said that Wise should reimburse the losses, pay interest and award £300 compensation. Wise denied it was responsible for what had happened and rejected the complaint.

One of our investigators reviewed the complaint and partially upheld it. He recommended that Wise reimburse 50% of the loss from the final successful payment of £3198.12 and pay 8% simple interest on that amount. He felt that Wise ought to have asked further questions about this transaction prior to it being processed and provided a tailored warning relevant to cryptocurrency scams. In his view, such steps would likely have prevented Mr A from making the payment and continuing with the scam.

However, the investigator also concluded that Mr A reasonably ought to have recognised the job offer was not genuine. Therefore, he determined that liability for the £3,198.12 payment should be shared equally."

Mr A accepted the investigator's findings but Wise disagreed. Its key arguments are summarised below:

- Under the terms of Mr A's debit card, Wise are not liable for any losses outside its control which occur on a separate platform.
- Wise is obliged to process debit card payments promptly given the nature of these transactions. It cannot hold or suspend them to ask additional questions, as the investigator suggested.
- Cryptocurrency purchases are not illegal, so Wise is not required to intervene in every transaction involving them. The payments successfully made on 11 January totalled less than £5000, which Wise does not consider a significant amount. Wise then appropriately intervened when, in its own words, a "concerningly large payment" was being attempted.
- Mr A had previously made payments to Crypto.com in November 2024, so he was familiar with the platform and was transferring funds to his own cryptocurrency wallet.
- Wise felt that a tailored scam warning would not have prevented Mr A from making the £3198.12 payment. It argued that his actions indicated a strong commitment to the scam and cited correspondence in which, after reporting the matter to Wise, he still suggested that he was actively seeking further funds through a bank loan to meet their demands.

The case has now been passed to me to make a final decision.

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 agree with the recommendation of the investigator and broadly for the same reasons. I will set out my key findings below.

Initial Considerations

There's no dispute that Mr A instructed Wise to make the payments. In broad terms, the starting position at law is that an Electronic Money Institution (EMI) such as Wise is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations 2017 (PSRs) and the terms and conditions of the customer's account.

The PSRs also do not offer specific protections from losses arising from authorised debit card payments like those subject to this case. In addition, references made by C to The Contingent Reimbursement Model (CRM) code and the Faster Payment Scheme (FPS) Reimbursement Rules in the complaint to Wise are not applicable to card transactions.

While the starting position is that Mr A is liable for payments he authorised Wise to make, I have also considered relevant law, regulatory rules and guidance, industry codes of practice, and what I regard as good industry practice at the time. In light of this, I consider it fair and reasonable that Wise should:

- Have been monitoring accounts and any payments made or received in order to counter various risks, including preventing fraud and scams.
- Have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud. This is particularly important given the increase in sophisticated fraud and scams in recent years, which EMIs like Wise are generally more familiar with than the average customer.
- Have acted to avoid causing foreseeable harm to customers. For example, by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products enabled it to do so.
- In some circumstances, take additional steps or checks before processing a payment, irrespective of the channel used.
- Have been mindful of common scam scenarios and how fraudulent practices are evolving, including the use of payments to cryptocurrency accounts as a step to defrauding customers, in order to provide tailored advice to address identified risks when deciding to intervene.

Should Wise have recognised that Mr A was at risk of financial harm from fraud?

With the above in mind, and in view of Mr A's account activity, I agree with the investigator that Wise should have taken further action at the point of the £3198.12 payment prior to processing it.

I acknowledge that Mr A had previously made payments to Crypto.com as Wise highlighted. However, past experience with a cryptocurrency platform does not necessarily eliminate future fraud risks involving it. I would also add that the seven previous payments made to the platform between 22-29 November 2024 were for relatively small amounts, with the largest being £170.89.

In my view, the activity on 11 January was markedly different and took place over a much shorter timeframe. After five relatively small payments, the amounts escalated significantly. By the time of the £3198.12 transaction— almost three times the previous payment of £1107.96 made less than an hour earlier—there had been six payments within roughly six hours to Crypto.com.

Given this pattern and the fact that the payments were directed to a recognised cryptocurrency exchange, I consider it fair and reasonable that Wise should have intervened at that point to review the activity and obtain further information from Mr A about the purpose of these transactions.

In its response to the investigator's findings, Wise argued that the nature of card payments prevents it from suspending or holding transactions to ask additional questions. However, this case shows that Wise can cancel payments when fraud is suspected. In my view, this demonstrates that there is nothing inherent in card payments that would have prevented Wise from reaching out to a customer to ask further questions about a transaction where fraud concerns existed before allowing an account to be debited.

The appropriate intervention and Mr A's actions

Since July 2023, when the FCA's new Consumer Duty came into force, there has been an obligation on firms to avoid foreseeable harms to customers. The Consumer Duty Finalised Guidance FG22/5 (Paragraph 5.23) gives an example of foreseeable harm:

"consumers becoming victims to scams relating to their financial products for example, due to a firm's inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers"

In light of this, and at the point of the £3198.12 payment attempt, I would have expected Wise to ask a series of questions designed to establish the actual scam risk and provide a tailored written warning.

Given that the payment was directed to a recognised cryptocurrency provider, those questions should have been specifically tailored to common scam scenarios involving cryptocurrency and their known characteristics. At the time these payments were made in January 2025, job scams involving cryptocurrency and conducted via popular instant messaging platforms such as Telegram were widespread and well documented.

Therefore, I would expect a firm like Wise to have both questions and warnings designed to identify and mitigate the risk of such a scam. For example, questions focused on some of the key indicators of job scams, such as promises of high pay in exchange for little work, unsolicited contact via social media or instant messaging platforms, and instructions to make payments to cryptocurrency exchanges or wallets as part of completing supposed tasks. These are well-recognised hallmarks of such scams, all of which were present in Mr A's case.

I have no reason to believe that Mr A would have answered dishonestly during such an intervention. Therefore, I am satisfied that had appropriate questioning taken place, his answers would likely have revealed he was the victim of a job scam, and Wise should have provided a tailored warning to deter him.

Wise argued that no warning would have prevented Mr A from making the £3,198.12 payment, given his subsequent attempts involving larger sums. I do not accept this, as those attempts occurred in circumstances where no warning had been provided to prompt him to consider the possibility that he was being scammed.

I have also considered Mr A's comments to one of the scammers which suggested that he was attempting to obtain a loan to meet their demands following the scam being reported to Wise. When asked about this, C said that Mr A was not actively seeking further funds and he only did this to keep the scammers engaged in view of the possibility that they could be traced.

I do not believe that Mr A was seriously contemplating making further payments to the scammers after he had reported his concerns to Wise. Shortly after these comments were made, Mr A did not engage any further with the scammers, despite repeated messages from them every day over the following week.

Although I question his decision to keep engaging with them, I note that Wise did not ask any questions about the scam he reported or provide relevant guidance—such as advising him to cease further communication with the scammers.

In line with what I've said already, I would need to be sufficiently concerned that Mr A's comments to the scammers demonstrate that he would have ignored a proportionate warning around job scams had it occurred and made the £3198.12 payment regardless. On balance of probabilities, I think it is likely that he would not have made any further payments to the scam had such an appropriate intervention occurred.

That said, I agree with the investigator that it is reasonable for Mr A to bear some responsibility for the losses arising from the payment that required further action by Wise. Although C argued that Mr A was vulnerable to the scam on medical grounds, no supporting evidence was provided when requested by the investigator, and C replied that this had not been medically diagnosed. Given this, and the circumstances overall here, I'm persuaded the 50% deduction remains fair.

Recovery

The chargeback scheme is a possible avenue to explore for recovery of funds made via debit card.

However, Mr A's payments were made to a legitimate cryptocurrency exchange, not directly to the scammers. For chargeback purposes, the merchant would therefore be the exchange, which fulfilled its contractual obligations by providing the intended service. The subsequent transfer of funds to the scammers falls outside the scope of a valid chargeback claim. On that basis, I don't think Wise could have recovered these payments once processed.

Compensation

Although Mr A accepted the investigator's assessment without the £300 compensation initially proposed by C, I considered whether compensation for inconvenience or distress was appropriate.

Scams of this nature are inherently distressing, and I do not doubt the significant impact on Mr A. However, the primary cause of that distress was the actions of the scammers. Wise could not reasonably have prevented all of the payments from being made, so I believe the recommendations set out below in view of the circumstances of this case represent a fair and reasonable resolution.

Putting things right

Wise must:

- Refund 50% of the losses from the £3198.12 payment; and
- Pay interest on the above amount at the rate of 8% simple per year from the date of this payment to 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 Mr A how much it has taken off. It should also give Mr A a tax deduction certificate if he asks for one.

My final decision

My final decision is that I uphold Mr A's complaint in part. Wise Payments Limited must put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 2 January 2026.

James Abbott
Ombudsman