

## Complaint

Mrs B is unhappy that Wise Payments Ltd didn't agree to refund her after she fell victim to a scam.

## Background

In late-2023, Mrs B was contacted in connection with a job opportunity. The role was flexible in terms of the hours expected and could be completed remotely. She was told that she would be asked to complete tasks on a platform maintained by the employer. The premise was that these tasks would assist clients of the employer with "app optimisation." Unfortunately, this wasn't a legitimate job opportunity. Mrs B had been targeted by a fraudster.

She was told that she would earn commission for each task completed. However, her account on the company's platform needed to be funded. She was asked to make payments to the company platform to enable her to earn and access the commission payments she thought she'd be entitled to. She made those payments in the expectation that she'd earn back significantly more in terms of commission.

She used her Wise account to make the payments in the table below. Each payment was made to an account belonging to a private individual and was made in connection with a peer-to-peer cryptocurrency transaction. In other words, Mrs B paid these individuals to transfer cryptocurrency that they held into her name. I understand she then transferred that cryptocurrency on into the control of the fraudsters and she was told that this was how she needed to fund her account.

|                 |         |
|-----------------|---------|
| 3 December 2023 | £121.29 |
| 3 December 2023 | £5.93   |
| 4 December 2023 | £695    |
| 5 December 2023 | £230    |
| 5 December 2023 | £200    |
| 7 December 2023 | £2,050  |
| 7 December 2023 | £2,660  |

Once she realised she'd fallen victim to a scam, she notified Wise. It didn't agree to refund her losses. Mrs B wasn't happy with that response and so she referred her complaint to this service. It was looked at by an Investigator who didn't uphold it. Mrs B disagreed with the Investigator's opinion and so the complaint has been passed to me to consider and come to a final decision.

## Findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services

Regulations (in this case, the 2017 regulations) and the terms and conditions of the customer's account. It's common ground that Mrs B authorised these payments and so she is presumed liable at first instance.

Wise isn't a signatory to the Lending Standards Board's Contingent Reimbursement Model Code (CRM Code), so it doesn't apply to these payments. Nonetheless, good industry practice required that Wise be on the lookout for account activity or payments that were unusual or out of character to the extent that they might indicate a fraud risk. On spotting such a payment, I'd expect it to take steps to protect their customer. That might be as simple as providing a written warning as part of the payment process or it might extend to making contact with the customer to establish the circumstances surrounding the payment.

We now know with the benefit of hindsight that Mrs B was falling victim to a scam. The question I have to consider is whether that risk ought to have been apparent to Wise given the information that was available to it. I've considered that question carefully and I'm not persuaded Wise could reasonably have been expected to identify the fraud risk here.

The earliest payments were of low value and wouldn't have appeared particularly risky. I don't think it would be practical or realistic to expect Wise to intervene in connection with payments of that value. In addition, while these payments were made to purchase cryptocurrency, that wouldn't have been apparent to Wise because the payments weren't being made to a cryptocurrency exchange. These were peer-to-peer transactions and, from the perspective of the firm, they could've been made for a whole range of potential purposes.

Mrs B was asked to provide some supplementary information in connection with several of these payments. Unfortunately, I can see that the information she gave was misleading. She told Wise that two of them were being made to pay a bill and one was a payment to friends/family. Wise could reasonably have taken that information into consideration when deciding whether there was a fraud risk associated with these payments. Its ability to identify the risk was, unfortunately, hamstrung by the misleading information that Mrs B provided.

I do appreciate what Mrs B has said about why she answered Wise's questions in the way she did. She says that she was following the instructions of her supervisor who told her what she needed to do to make sure the payments weren't held up by the firm. However, the consequence of her answering its questions in the way she did was that it had no realistic chance of spotting that she was at risk of financial harm due to fraud.

For the sake of completeness, I've also looked at whether Wise did everything it could in respect of recovering Mrs B's money. But as these were payments made in connection with legitimate purchases of cryptocurrency from third parties who weren't connected to the scam, I don't think there was anything it could've done to recover her funds.

I don't say any of this to downplay or diminish the fact that Mrs B has fallen victim to a cruel and cynical scam. I have a great deal of sympathy for her and the position she's found herself in. Nonetheless, my role is to look at the actions and inactions of Wise and I'm satisfied it didn't do anything wrong here.

### **Final decision**

For the reasons I've explained above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs B to accept or reject my decision before 25 July 2025.

James Kimmitt  
**Ombudsman**