

The complaint

Miss D complains that Wise Payments Limited didn't do enough to protect her from the financial harm caused by an investment scam company, or to help her recover the money once she'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

Miss D was contacted on WhatsApp by someone who I'll refer to as "the scammer" who claimed for work for a company I'll refer to as "G". The scammer told Miss D about an opportunity to make some extra income which would require her to complete tasks via G's online platform.

Miss D believed the opportunity was genuine because the platform was professional looking and could be accessed by an app. G also had a social media presence, and she was sent letters of guarantee signed by the directors of the company which satisfied her the company was genuine.

The scammer told Miss D that G was looking to increase the marketing exposure of certain products and she would receive 1-5% commission for each task according to the value of the product. She was told to complete a short training course and added to a WhatsApp group with other workers who shared their successes.

The scammer told her to pay for each task by making payments via a cryptocurrency exchange company I'll refer to as B, before transferring it to G's platform. Between 17 November 2022 and 24 November 2022, she made fourteen card payments to B totalling \$2,978 and £25,134.14 from her Wise account.

Miss D generated an income and felt motivated because the scheme was straightforward. She paid increasing amounts so she could finish tasks and withdraw her profit, but when she was unable to make a withdrawal, she contacted customer service and was told they'd help her out with money to cover the packages. Miss D told the scammer she could pay for more tasks once she received her student loan. But on 11 January 2023, she was removed from the WhatsApp group and when she tried to make a withdrawal, her account was empty.

Miss D contacted Wise to report the scam and to complain that it should have identified the payments as unusual and performed additional checks, which could have uncovered the scam and prevented her loss.

But Wise refused to refund any of the money. It explained that payments are generally considered completed once the funds are loaded to the recipient account, regardless of what happens from there, so there would be no prospect of a successful chargeback request. It explained it is a Money Remittance Service and wouldn't be involved in disputes between senders and recipients as it can't control or monitor activities after a transaction has left its system. It said it had attempted to recall the money from B on 12 February 2023, but it didn't

receive a response and there was little else it could do to because the payments were 3DS - approved.

Miss D wasn't satisfied and so she complained to this service with the assistance of a representative. The representative said Miss D hadn't previously invested in cryptocurrency and hadn't made many payments over £1,000, so the activity was unusual. They said she mainly used the account while on holiday and on 22 November 2022 she paid £2,580 and £5,000 to B, which should have raised concerns as the payee was a cryptocurrency merchant.

They said Wise should have contacted Miss D to ask questions about the payments and had it done so, she'd have told it the payments related to a job opportunity which she'd learned about on WhatsApp. Wise could then have identified that a scam taking place and been able to advise Miss D about what was happening, and she wouldn't have lost any more money.

Wise has further commented that the obligation of ensuring the legitimacy of the recipient was Miss D's and she was using her account in the normal way - i.e. funding the balance from her bank account, and then using that money to spend with her debit card. And even though she was moving money from her Wise account over a short period, B was a legitimate merchant, so it didn't believe the payments were unusual.

Our investigator thought the complaint should be upheld. He accepted the first few payments were to a new payee which was a cryptocurrency merchant, but he didn't think they were high enough to have triggered a warning from Wise. But he thought it ought to have been concerned when Miss D made the payment of £5,000 on 22 November 2022. And he was satisfied that if Wise had contacted her and questioned her about the payments, it is likely she'd have explained why she was making the payments. It could then have provided a scam warning which would have changed the outcome, so it should refund the money she lost from that point onwards.

However, he explained that although this was a sophisticated scam, it wasn't reasonable for Miss D to have thought this was a legitimate job as there wasn't a plausible reason to pay funds to an employer or for G to have offered to make payments on her behalf, so he thought the settlement should be reduced by 50% for contributory negligence.

W has asked for the complaint to be reviewed by an Ombudsman. It doesn't agree it should have intervened on 22 November 2022 arguing that before making the payment of £5,000 Miss D had added £5,490 to the account from another account in her name suggesting she was preparing to send a higher amount. And she had made previous payments to B, so the payment wasn't out of character.

It has further explained that its customers may need to change spending behaviour and send large payments to new recipients, which what its product is designed for and how its used by its customers. It has said balances are often used to fund outbound payments and funds are not always left sitting in accounts as with traditional bank accounts.

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 reached the same conclusion as our investigator. And for largely the same reasons.

I'm satisfied Miss D 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although she didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of her bank account, Miss D is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although she didn't intend her money to go to scammers, she did authorise the disputed payments. Wise is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

I've thought about whether Wise could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to a genuine cryptocurrency exchange company. However, Wise had an obligation to be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have intervened to warn Miss D when she tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Wise to intervene with a view to protecting Miss D from financial harm due to fraud.

The payments didn't flag as suspicious on Wise's systems. I've considered the nature of the payments in the context of whether they should have triggered an intervention from Wise and I think they should. All the payments were to a legitimate cryptocurrency exchange company, and the initial payments were for lower amounts, so it wasn't unreasonable that Wise didn't intervene. But on 22 November 2022, Miss D made a payment of £5,000 which should reasonably have triggered an intervention.

This is because, even though this was a legitimate cryptocurrency merchant which Miss D had paid several times since 17 November 2022 and there were two payments totalling £5,490 into the account, £5,000 is a significant amount and ought to have raised concerns, particularly as there wasn't a history of larger payments on the account. So, I think Wise missed an opportunity to intervene.

Wise should have contacted Miss D to ask her about the purpose of the payment. And as there's no evidence she'd been coached to lie, I think it's likely she'd have told it that she was making payments in respect of a job opportunity she'd learned about via WhatsApp for which she expected to receive commission.

With this information, I would expect Wise to have identified that the job had the hallmarks of a scam and to have discussed with her the nature of the checks she'd undertaken and to give some advice on additional due diligence. I would also expect it to have warned Miss D that there were several red flags present including the fact she'd been contacted on social media and required to make payments to a company in cryptocurrency.

I haven't seen any evidence that Miss D was keen to take risks with her money and so if Wise had warned her that this was probably a scam, I think it's likely that she'd have thought twice about making any more payments. Because of this, I think it missed an opportunity to intervene in circumstances where to do so might have prevented her loss. Consequently, I think it should refund the money she lost from 22 November 2022 onwards.

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence and these circumstances are such that I think Miss D should share some responsibility for her loss.

Miss D was contacted on social media by someone claiming to be offering an opportunity to make money by completing tasks in return for commission. While this isn't necessarily alarming and I accept this was a sophisticated scam in that G appeared to have a website and a trading platform which was accessible via an app, Miss D ought to have questioned where the scammer got her details, why she was being asked to pay money to G using cryptocurrency and why she wasn't given any employment documentation such as a contract.

So, I think the settlement should be reduced by 50% for contributory negligence.

My final decision

My final decision is that Wise Payments Limited should:

- refund £21,057.
- this settlement should be reduced by 50% to reflect contributory negligence.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

If Wise Payments Limited deducts tax in relation to the interest element of this award it should provide Miss D with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss D to accept or reject my decision before 15 December 2023.

Carolyn Bonnell
Ombudsman