

## The complaint

Mrs K complains that Wise Payments Limited (“Wise”) won’t refund over the money she lost to an investment scam.

## What happened

The details of this complaint are well known to both parties, so I won’t repeat everything again here. In brief, Mrs K saw an advert for a sports betting company that I will call B on a social media website. Mrs K contacted B and it was explained to her that B could offer guaranteed returns on betting on the incorrect scores of football matches.

Mrs K was then persuaded to make the following payments firstly to a crypto exchange and then the funds were forwarded onto B.

Transaction Number	Date	Amount	Type of Payment
1	25 March 2022	£348	Debit Card
2	25 March 2022	£200	Debit Card
3	25 March 2022	£124	Debit Card
4	30 March 2022	£1,696	Debit Card
5	30 March 2022	£3,796	Debit Card
6	31 March 2022	£198	Debit Card
7	2 April 2022	£44	Debit Card
8	3 April 2022	£118	Debit Card
9	3 April 2022	£44	Debit Card
10	6 April 2022	£198	Debit Card
11	7 April 2022	£41	Debit Card
12	7 April 2022	£4,996	Debit Card
13	8 April 2022	£50	Debit Card
14	8 April 2022	£1,596	Debit Card

When B’s platform disappeared Mrs K realised, she had been scammed.

Mrs K complained via a representative to Wise and requested that she be refunded the payments that she made as they believe that had Mrs K been warned by Wise during the scam the scam would have been prevented. Wise declined to do this.

Our investigator upheld this complaint. She thought that Wise ought to have questioned Mrs K about payment 5 and provided her with a scam warning. The investigator thought that, had that happened, Mrs K would not have carried on with the scam. She therefore thought that Wise should refund 50% of the transaction made from this transaction onwards as she thought that Mrs K contributed to her own loss.

Mrs K agreed but Wise did not respond and therefore this complaint was passed to me to issue a 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.

It isn't in dispute that Mrs K has fallen victim to a scam here, nor that she authorised the disputed payments she made to the scammer. The payments were requested by her using her legitimate security credentials provided by Wise, and the starting position is that Electronic Money institutes (EMI's") ought to follow the instructions given by their customers, in order for legitimate payments to be made as instructed.

However, I've considered whether Wise should have done more to prevent Mrs K from falling victim to the scam, as there are some situations in which it should reasonably have had a closer look at the circumstances surrounding a particular transaction. For example, if it was particularly out of character for that account holder. I also note that Wise does have the provision in its terms and conditions to stop payments if it believes they are fraudulent.

In this instance, I do not have a payment history of Mrs K but that said payment 5 was enough in my view to have prompted an intervention from Wise. It represented transactions of over £5,000 in one day which I feel based on the limited information that I have would be considered as unusual.

I think by March 2022 Wise should really have been aware of the dangers of crypto scams and given the pattern of payments before and the size of this transaction I'm satisfied this payment ought reasonably to have been considered as unusual and triggered an intervention by Wise. I think that Wise should also have been aware that multiple payments in quick succession to a crypto exchange should really have alerted Wise that something unusual was going on.

Wise is aware of the typical patterns of scams like this – that customers often move money onto a crypto exchange account in their own name before moving it on again to scammers; and that scams like this commonly take place with multiple payments. So, I think Wise should really have intervened during payment 5 to question what the payment was for.

I also appreciate that Mrs K's loss didn't materialise directly from her Wise account in these circumstances. But even though she was transferring funds to a crypto exchange account in her own name, I still think that Wise ought to have taken a closer look at this payment – given the significant risk of fraud associated with cryptocurrency investments at the time.

The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018. And by January 2019, cryptocurrency scams continued to increase in frequency. So, by the time Mrs K started making her investments in 2022, it is reasonable to say Wise ought to have had a good enough understanding of how crypto scams works – including the fact that their customer often moves money to an account in their own name before moving it on again to the fraudster.

Therefore, I'm satisfied that Wise should've had mechanisms in place to detect and prevent this type of fraud at the time Mrs K was making this payment, and that it should have led to it intervening to ask further questions about the payment in question.

I would expect Wise to have intervened and asked Mrs K who the payment was for, what it was for, and for the context surrounding the payment - it could, for example have, asked how she had been contacted, whether she'd parted with personal details, whether she was being helped by any third parties e.g. a broker, and how she had come across the "investment" in this case via an advert.

I recognise that if an intervention by Wise had taken place, it likely would've identified that the payment was going to the consumer's own account with the crypto exchange in question. But I don't think the conversation should have stopped only on the basis that the money appeared to be going somewhere safe and within the consumer's control.

I say this because, by the time Mrs K made these payments, Wise ought reasonably to have had a good enough understanding of how these scams worked and to have been able to identify the risk of harm occurring to its account holders from fraud. This includes the consumer often making a number of purchases of crypto assets in a relatively short space of time or a consumer repeatedly sending money to a platform where the money is subsequently moved on to or taken by the scammer. So, it is with this in mind that I think Wise ought to have probed further about the nature and context of the payments Mrs K was making.

I have no reason to believe Mrs K wouldn't have been open with Wise, I think she would have taken its intervention seriously and I can't see that she was being coached by the scammer. So, I think Wise would have quickly learned from its conversation with Mrs K the basic background to the payment instruction – that she was intending to buy cryptocurrency which would then be sent onto what she thought was a sports betting investment in which she would receive guaranteed returns betting on the incorrect scores in football matches.

In light of this, I think Mrs K's losses were foreseeable to Wise, despite the payments on the face of it not leaving her control. And I'm satisfied that, had Wise asked relevant questions of Mrs K, it would have been apparent that she was falling victim to a scam. In other words, but for Wise's failure to make reasonable further enquiries, it would have been on notice that there was a very high chance that Mrs K was going to suffer financial harm from fraud.

Had Wise provided Mrs K with a warning, it would have likely alerted her to the common issues arising in relation to cryptocurrency scams. I think this, in turn, would have led Mrs K to question whether she was in fact dealing with a legitimate business and would have likely stopped Mrs K from making any further payments.

As a result, I believe Wise should refund the payments Mrs K lost to the scam from payment 5.

There's a general principle that consumers must take responsibility for their decisions. And I have duly considered whether Mrs K should bear some responsibility by way of contributory negligence. In the circumstances, I'm satisfied she should do so in this case.

In this instance it is not clear what research Mrs K did. But any basic research would have made guaranteed returns on sport betting seem more than a little unrealistic and should have caused her some concern as to whether what she was being promised was real. I also can see that she had some concerns about the legitimacy about B early on in the scam, yet she chose to proceed despite these reservations.

Therefore, I'm satisfied that Mrs K's lack of due diligence and that she proceeded despite her reservations means that she should share responsibility with Wise. Because of this, I'm satisfied a 50% deduction is fair and reasonable in the circumstances

### *Recovery*

In relation to recovering the funds, I don't think that Wise could have recovered the debit card payments. The main way to recover the payments would be to attempt a chargeback but I don't consider Wise ought to have attempted a chargeback claim, as Mrs K made payments to get crypto and she seems to have received this before she forwarded it on to B. So, she got what she paid for.

### **Putting things right**

For the reasons given above, I uphold this complaint in part and direct Wise Payments Limited to:

- Refund the payments Mrs K lost to the scam from and including transaction 5, less a deduction of 50% in recognition of Mrs K's own contributory negligence towards her loss.
- Pay 8% simple interest per year on this amount, calculated from the date of loss until the date of settlement, minus any applicable tax.

### **My final decision**

My final decision is that I uphold this complaint in part and direct Wise Payments Limited to pay the redress outlined above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs K to accept or reject my decision before 14 March 2024.

Charlie Newton  
**Ombudsman**