DRN-4674401

The complaint

Mr W complains that Wise Payments Limited (Wise) won't refund money he lost in a recovery scam.

What happened

What Mr W says:

Mr W was the victim of an investment scam – which took place between June 2022 and January 2023. He lost more than £109,000 – that complaint has also been brought to this service. Within that sum, he paid £3,770 to a 'recovery agent'.

In January 2023, Mr W realised he'd been scammed. He then saw an advert on Facebook for a Scam Recovery service – which claimed to be a specialist in crypto related schemes. He linked up with the Swedish company and corresponded via WhatsApp. He signed various official documents and gave proof of ID.

He was asked to pay upfront fees, which he did - in crypto currency. The agency claimed to have traced the funds to an account in Russia and Mr W paid a further fee. He got several promises of payment, but nothing arrived and his WhatsApp messages then went unread.

He then realised he had been the victim of a further, recovery scam – he said it was likely linked to the original scam. He says he paid the recovery agent almost £20,000 – £3,770 from his other bank account, £3,867.27 from a credit card account - and £13,357 from his account with Wise.

The payments from Mr W's Wise account were:

Date	Payment	Amount
6 February 2023	Debit card – crypto exchange	£3,500
3 March 2023	Debit card – crypto exchange	£3,457
19 April 2023	Debit card – crypto exchange	£6,400
Total		**£13,357**

Mr W says the recovery agent operated under the disguise of what appeared to be a genuine law firm. He believed they were genuine and were trying to help him.

Mr W says Wise should've intervened to protect him. He had only just opened his account and therefore the payments were unusual. If Wise had contacted him and told him he was potentially being scammed, he would not have made the payments. He says he would accept a refund of 50% of the money he paid.

What Wise said:

Wise said the payments were properly authorised. The firm said Mr W should contact the merchant (the crypto exchanges) to ask for a refund.

Wise said their customers frequently make similar large payments using their Wise debit cards – often when there was little or no previous account history. In this case, Mr W had only recently opened his account, so there wasn't any history to compare the payments to.

Wise didn't refund any money.

Our investigation so far:

Mr W brought his complaint to us. Our investigator didn't uphold it. She said:

- Wise should've intervened in the first payment because it was unusual. This was a newly opened account and the payment was to a crypto related recipient.

- Wise should've provided a tailored warning to Mr W but didn't.

- However, even if Wise had done so she didn't think it would've made a difference. She could see from the WhatsApp chats that Mr W had complete trust in the scammer. For example, he gave the scammer the security words needed to open one of the wallets.

- And, one of the crypto exchanges had blocked Mr W's account and asked some questions, but Mr W still went ahead.

Mr W (through his advisors) didn't agree. He said:

- Wise should have intervened, especially as this was a new account with no history – the first payments were those related to the scam.

- How could it be stated with any certainty that any intervention would not have had an effect?

Mr W asked that his complaint be looked at by an ombudsman, and so it has come to me.
(continued)

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'm sorry to hear that Mr W has lost money in a cruel scam. It's not in question that he authorised and consented to the payments in this case. So although Mr W didn't intend for the money to go to a scammer, he is presumed to be liable for the loss in the first instance.

So, in broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case.

But that is not the end of the story. Taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Wise should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and 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 (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

I need to decide whether Wise acted fairly and reasonably in its dealings with Mr W when he made the payments, or whether it should have done more than it did. I have considered the position carefully.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) provides for refunds in certain circumstances when a scam takes place. But – it doesn't apply in this case. That is because Wise hasn't signed up to the code. And in any case, it applies to faster payments made to another UK beneficiary– and in this case, the payments were made to Mr W's own accounts with the crypto exchange and using a debit card.

Having looked at what happened here - the amounts were not of a high enough value to expect Wise to have intervened - Electronic Money Institutes (EMIs) such as Wise are typically used for larger payments, so the amounts in dispute here wouldn't be considered suspicious – even given that the account was a new one.

I asked Wise what reasons Mr W gave for using the account when he opened it – and he told Wise it was for 'buying goods or services abroad'. So – the payments in question were in line with that.

And – the payments were spaced far apart. There were three payments over ten weeks. This isn't the typical pattern of a scam – where payments are normally made in rapid succession.

So on balance, this means that in this case, there being no obvious other concerning factors that were evident, we take the view that Wise didn't need to send a tailored warning to Mr W or contact him in some other way. So, I disagree with our investigator in this respect.

And therefore, on that basis, I am not upholding this complaint.

Recovery of funds: We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I didn't see any evidence that Wise had done so.

But in this case, the funds went from the bank account to a crypto currency merchant and the loss occurred when crypto was then forwarded to the scammers. In this case, as the

funds had already been forwarded on in the form of cryptocurrency there wasn't likely to be anything to recover.

I'm sorry Mr W has had to contact us in these circumstances. I accept he's been the victim of a cruel scam, but I can't reasonably hold Wise responsible for his losses.

My final decision

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 1 February 2025.

Martin Lord
Ombudsman