DRN-4545528

The complaint

Mr S complains that Wise Payments Limited (Wise) won't refund the money he lost when he fell victim to a scam.

What happened

Mr S says he won some cryptocurrency from an online game many years ago, when it was worth a lot less. He didn't know where it was held and had tried to locate it over the years – but hadn't succeeded. So when he got an email saying his cryptocurrency had been located, he believed it. Unfortunately, it was a scam.

After Mr S replied to the email, he received a follow-up message via WhatsApp. He says he was sceptical at first, but was reassured when the person sent him photographs of herself and her family. She got him to provide documents to verify his identity. She then told him he needed to send funds to the account they had located for him in order to reactive it, given the time that was passed. Mr S says he was sent a link to register with a (genuine) cryptocurrency platform – "C". And he sent £1,000 from Wise to that account on 5 July 2022.

Mr S was subsequently contacted by another individual claiming to be from the company recovering his funds. Mr S says he was asked to download remote access software so they could help with this. He thinks this allowed the scammers to get access to his Wise account, send payments to his account with C, and then send the funds on from there.

On 6 July 2022, Wise asked Mr S to provide a selfie as verification, seemingly because it had fraud concerns. This was provided. On 7 July 2022, Mr S reported a number of transactions as unauthorised. When Wise attempted to follow up, it got a response from Mr S's email address saying to allow the transactions – "even Cryptos".

As well as the payments to C, payments were also sent to "B" – the company the scammers were impersonating. But B identified the payments as suspicious and returned them. There was also one payment made to another cryptocurrency merchant (S), and a payment to an individual, which Mr S says he didn't consent to.

Mr S says he realised it was a scam when the individuals gave him an invoice saying he needed to pay a further amount. So he reported this to Wise, as well as C and B. But Wise wouldn't agree to refund him. He therefore referred the matter on to our service.

Our investigator thought the payments should be considered authorised. While she thought Wise ought to have issued a tailored scam warning in response to the account activity, she wasn't persuaded this would have uncovered the scam – as Mr S's explanation of what happened suggests this would have been seen by the scammers rather than him. But she did think Wise ought to have stopped the last two payments, as these occurred after Mr S had notified it of the scam.

Mr S appealed. He disputed that he participated in the payments. He says he was fully under the control of the scammers, and Wise ignored the irregular account activity. He also highlighted some scam payments he had missed in his in initial dispute.

Wise has consented to us considering all these payments, as set out in the table below (please note those in italic mean no fraudulent loss was directly incurred). Initially, it agreed with the investigator's outcome. But it has subsequently told us it won't agree to refund the card payment on 13 July 2023 as it was authenticated using '3DS' verification.

Date	Amount	Account	Type	Recipient	Additional notes
05/07/2022	£1,000.00/ €1,168.26	Personal Euro account	Card	C (crypto merchant)	
06/07/2022	*$10.00/ €9.81*	*Personal Euro account*	*Card*	*B (crypto merchant)*	*Returned by B 13/7*
06/07/2022	£9,900.00/€1 1,606.20	Personal Euro account	Card	C	
06/07/2022	*€20,000.00*	*Personal Euro account*	*Transfer*	*Mr S's business account*	*Unsuccessful: returned by Wise 8/7*
07/07/2022	*€3,000.28*	*Personal Euro account*	*Transfer*	*B*	*Returned by B 13/7 (minus €0.28 Wise fee)*
08/07/2022	*€10,000.00*	*Personal Euro account*	*Transfer*	*Mr S's business account*	*Source of business account transfer 11/7*
11/07/2022	£10,000.00/ €11,864.70	Personal Euro account	Card	C	
11/07/2022	€10,000.00	Business Euro account	*Card*	C	
12/07/2022	€8,300.00	Personal Euro account	Card	C	
13/07/2022	£2,080.00/ €2,740.18	Personal Euro account	Card	S (crypto merchant)	
13/07/2022	€ 584.91	Personal Euro account	Transfer	Individual	

As no agreement was reached, the case was passed to me for review. I issued my provisional decision in December 2023 explaining I was minded to direct Wise to refund some, but not all, of Mr S's loss for the following reasons:

> *I've started by considering whether, in line with the relevant regulations – the Payment Services Regulations 2017 (PSRs) – the payments should be considered authorised. That is relevant as, in broad terms, account holder are generally liable for payments they authorise – but the account provider would generally be liable for unauthorised payments.*
>
> *Under the PSRs, whether the payments were authorised comes down to whether Mr S, or someone acting with his authority, completed the agreed payment steps (such as accessing the app and entering the details for a transfer, or entering/using saved card details and confirming the payment in the app through a notification, or by entering a code sent to his registered phone).*
>
> *Mr S confirms he made the first payment (£1,000 to C) – thinking he needed to pay this to release his cryptocurrency. While he disputes authorising the subsequent payments, on balance, I think he did. That means I think Mr S either completed the payment steps himself – or gave the scammer access to complete the steps. I accept this was due to him being tricked. But that doesn't affect authorisation as defined by the PSRs.*

I've come to this conclusion because:

- *For the transfers sent to B and C, Wise has provided information to show these were completed using Mr S's phone. My understanding is the operating system he uses means remote access software can only be used to view the screen – and not to take control. And it can only be used when the device holder is online/active. So I'm not satisfied what Mr S told us about the use of remote access software explains how the scammers could have made all these transactions without his involvement.*

- *I've seen records of an email exchange between Mr S and B. I'm satisfied these messages were sent by him as they post-date, and discuss, the scam. In it, he explains he was contacted by someone "claiming to purchase for me Bitcoin and will deposit in my wallet". And in another he says "I have purchased many Bitcoins in the last 8 days paid for from my debit card… I am so worried if I have been scammed". These messages further suggest Mr S was aware of and agreed to the transactions.*

- *While he contacted Wise on 7 July 2002 to report the cryptocurrency payments as unauthorised, this included the first payment of £1,000 sent to C – which Mr S has subsequently confirmed he authorised. So there is a contradiction here. He also disputed other payments which it now appears to be accepted he authorised. Additionally, when Wise replied asking for further information about the dispute, it received a reply from Mr S's email address saying to allow all the transactions.*

- *I appreciate Mr S says the scammers had access to his email. I accept this is plausible. They could have remotely accessed his computer, which could have allowed them to take control. But I wouldn't say there is a noticeable difference in tone between the emails sent to various parties which we know were sent by Mr S (as they mention the scam) and those which he says were the scammer.*

- *At the least, Mr S was aware the scammers had access to his accounts and were making payments. Unless he took steps to revoke that access, we would consider the payments made by the scammers to be authorised - even if he wasn't involved in each specifically. Without removing their access, he was, in effect allowing them to continue acting as his agent.*

- *Although Mr S then called Wise on 12 July 2022 to again dispute the payments as unauthorised, I have difficulty reconciling that with his prior contact and his emails to B. I think it's more likely he was reporting them because he knew, or suspected, they were the result of a scam – rather than because he was thinking about whether they met the PSR definition of authorisation.*

- *Furthermore, when Wise sent a follow-up email, it got a reply from his address which said: "Please don't take any action now just freeze everything for now ok until further request form me, they might genuine company...". I consider it likely this was sent by Mr S, as I can't see why the scammers would have asked Wise to freeze the account. And I think they would have been more unequivocal in asserting the payments/company was genuine.*

- *This email suggests Mr S was still dealing with the scammers after reporting his concerns to Wise, and that they managed to persuade him they were legitimate. I therefore consider it more likely the later payments were authorised by Mr S due to him being further manipulated/tricked by the scammers.*

- *This is supported by the information I have about how the payments were authenticated/processed. It appears the card payment required 3DS, so would have needed access to Mr S's app and/or text messages. It also appears his phone was used in connection with the transfer. As set out above, it seems unlikely a scammer would be able to do this via remote access.*

In line with the PSRs, Wise is expected to execute authorised payment instructions without undue delay. However, there are circumstances when it might be appropriate for Wise, as an authorised Electronic Money Institute (EMI), to identify a fraud risk – and to therefore take additional steps before processing a payment. That might occur as when the payment is significantly unusual or uncharacteristic when compared to the normal use of the account.

I don't think the first two scam payments presented an obvious fraud risk. While connected to cryptocurrency, they were sent to legitimate merchants. We expect firms to be aware legitimate cryptocurrency merchants can be used in scams like this, and to factor that into their anti-fraud measures. But we wouldn't expect a firm to intervene on every payment going to a genuine cryptocurrency merchant. And I don't think the payments looked otherwise uncharacteristic or concerning.

However, it seems Wise did have concerns around the time of the third payment (£9,900.00 to C on 6 July 2022). That's because it requested selfie ID from Mr S before it would approve any pending transactions to C. That suggests it did have fraud concerns regarding this payment. I can see why. Based on the records Wise has provided, the payment looks uncharacteristic – as Mr S didn't generally use his account for payments of this size. I also think it looked concerning that he was paying C such a large amount after having paid them for the first time just the day before.

While I understand why the selfie ID would have given Wise reassurance it was likely Mr S requesting the payment, I'm not persuaded that was a proportionate response to the risk identified. As mentioned above, we do expect firms to be aware of the prevalence and characteristics of cryptocurrency scams. Given this knowledge, and the concerning account activity, I consider it remiss that Wise didn't reach out to Mr S to find out more about why he was making the payment.

As explained above, I don't think the scammers had independent access to/control of Mr S's account. So by reaching out via in-app chat, or calling him, I think Wise would have been able to speak to him directly. I've not seen any indication he had been coached on what to say if questioned about the payments. I therefore consider it likely that, if asked, Mr S would have explained what he was doing. And I expect Wise would have realised this was a scam.

Mr S has told us he had his own concerns and suspicions. So I think he would have listened to a warning from Wise – meaning this would have successfully prevented his further losses.

I also think there were further alarming factors which Wise didn't respond to adequately. It was reasonable for it to go back with further questions about the payments he disputed on 7 July 2022. But the response it got just said:

"Hello wise
Allow online transfers and transactions even Cryptos. Thanks you Regards"

As its email reply said, this is "completely not related to the email [Wise] sent". But it closed the incident down after receiving another message from the email addressing saying "Halo wise thanks". I think Wise had cause for concern based on those messages. It seemed clear email contact wasn't getting to the bottom of the dispute, yet it took no further action to ensure Mr S wasn't at risk.

Additionally, Mr S called Wise on 12 July 2022 to report the payments as unauthorised. As mentioned above, he then emailed to say he thought the company might be genuine. But he said to "freeze everything" until he got back in touch. Wise didn't do that, and two further payments were made.

While I appreciate there was some confusion around the messages, Wise knew Mr S had downloaded remote access software, and that he was disputing cryptocurrency payments. I think it was remiss that it therefore didn't block his account, in line with his instructions, until it had spoken to him further to understand the situation.

I therefore think Wise's failures to respond appropriately to the fraud risk led to Mr S's loss. I think it holds liability from the third scam payment onwards – as I think it missed an opportunity to uncover the scam and prevent Mr S's further losses at this point.

However, I've also considered whether Mr S is partly to blame for his loss by way of contributory negligence. For the following reasons, I think it would be fair to expect him to share liability for his loss along with Wise:

- *He has told us he had misgivings from the point of the initial contact. I'm not persuaded it was reasonable for him to rely on the messages and pictures sent by the scammer as relevant to assessing their legitimacy.*

- *While I think Wise ought to have been able to uncover things earlier, I also think Mr S's contact made this more difficult. Such as his disputing payments as unauthorised that were unrelated to the scam, as well as disputing a scam payment it's clear he completed himself.*

- *Mr S appears to have continued engaging with the scammers even after being concerned enough to call Wise about what had happened. As following this, he messaged Wise to say the company might be legitimate. While I still think Wise should have prevented these payments, I think the loss could also have been avoided by Mr S.*

In light of this, I think it would be fair to expect Wise to refund 50% of the loss Mr S incurred as a result of the scam from payment three (£9,900.00 to C on 6 July 2022) onwards. Along with 8% simple interest per year, to compensate him for the loss of use of the funds.

I appreciate there was likely a vulnerability aspect affecting how things unfolded. But prior to the scam, I can't see this was something Wise ought to have been aware of, so it wouldn't have known if he needed a different level of support. And despite any vulnerabilities, Mr S's own testimony suggests he was still able to identify the warning signs. So I think a 50% deduction is fair.

And while I also appreciate Mr S's contact made it more difficult to establish what was happening, I'm conscious that at no point (including when Mr S rang Wise) does it appear Wise asked about the reason for the payments or how he came to be dealing with the company they related to. And I think that would have been the key to uncovering the scam.

I invited both parties to provide any further comments or evidence they wanted me to consider before I made my final decision. Wise hasn't replied, and the deadline I set for further submissions has now passed.

Mr S provided some further commentary for me to consider, which I've summarised below:

- There is new legislation coming into force that will make it easier for victims of authorised push payment (APP) fraud to get their money back. Mr S also highlights legislation and rules that are currently in place.
- All his savings with Wise were emptied within 13 days due to the scammers, having never made payments before. And they continued after he had raised his complaint. The rapid rate of the transactions should have alerted Wise.
- The scammers "strongly guided and forcefully led" him. They told him he had a wallet containing over £50,00 ready to cash in and provided evidence from companies house for B, contributing to him trusting them.
- He has highlighted the vulnerable circumstances he was in due to his health and age.
- He says he didn't authorise the card payments. That was done by the scammers, and, if needed, they got him to agree with "false transfers and demands".

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 come to the same conclusion as I did in my provisional decision. This is largely for the reasons, which are set out above and form part of my final decision. But I'll go on to address the points Mr S has raised in response to my provisional findings.

I'm aware of the legislation being introduced that Mr S has been referred to. As it isn't currently in force/wasn't in force at the time of the payments, that doesn't have a bearing on my findings.

However, as my provisional decision explained, we do still expect payment services providers to monitor for indications of fraud. And we can hold them liable for losses their customers incur due to them not meeting the expected standards.

Mr S says Wise should have been concerned by the volume of payments. I agree. Wise did, in fact, identify and respond to a fraud risk on 6 July 2022. It is precisely because I've found it responded to this risk inadequately, in a way that materially affected Mr S's loss, that I have held Wise liable from that point.

That said, I do think Mr S should share liability – by way of contributory negligence. I have considered what he has said about his circumstances at the time, and why he trusted the scammers. These are factors I considered and explained in my provisional decision. For the reasons I have already given, I still consider it fair to hold Mr S party to blame – which is why I have decided a 50% refund is fair.

Mr S says he didn't authorise any of the card payments. And any steps he undertook were due to being tricked. But earlier, he said he didn't complete the steps at all, and that they must have been done via remote access. So this seems to be a further change in his account of what happened. And his current explain also doesn't account for why he messaged B and said he *had* been purchased cryptocurrency.

Overall, for the reasons I've explained, I do consider it likely Mr S consented to the payments. I have therefore decided to make the same award as I proposed in my provisional decision.

My final decision

For the reasons given above, I uphold this complaint. Wise Payments Limited must refund Mr S 50% of the scam payments, from payment three onwards, along with half of any fees charged in relation to these. It should also pay 8% simple interest per year on this amount, running from the dates of payment to the date of settlement.

Wise Payments Limited must pay this compensation within 28 days of the date on which we tell it Mr S accepts my final decision.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 6 February 2024.

Rachel Loughlin
Ombudsman