

## **The complaint**

Mr M complains that Wise Payments Limited didn't do enough to protect him from the financial harm caused by an investment scam, or to help him recover the money once he'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.

Mr M was introduced by a colleague to someone who claimed to work for a cryptocurrency exchange company which I'll refer to as "B". The person told Mr M he could make money by investing in cryptocurrency and put him in touch with a senior broker, who I'll refer to as "the scammer".

The scammer asked Mr M to submit ID documents and to download AnyDesk remote access software to his device. From there he guided him to open an account with B and told him he could make 10% to 20% return per month, he could start with a small investment and, he'd be able to make withdrawals at any time.

Mr M checked the scammer's social media profile, noting he had B's logo as the profile picture. He sounded professional on the phone and the background noise sounded like a financial exchange. He used technical language and seemed knowledgeable and experienced in cryptocurrency investments.

The scammer asked Mr M to first purchase cryptocurrency and then load it onto an online wallet. Between 10 May 2023 and 26 May 2023, the scammer accessed Mr M's laptop and made five payments totalling £20,925. Mr M was given access to a portal where he could monitor his investments on the trading platform and see his deposits. He was continually asked for more payments to keep the returns high and eventually he realised the investment was a scam when he tried to make a withdrawal and was told he'd first have to make a payment of £9,000.

Mr M complained to Wise, but it refused to refund any of the money he'd lost. It said the initial debit card payment was verified by 3DS and the faster payments were to an account in Mr M's own name, so it had no reason to believe the payments were fraudulent. It said it can only monitor activities related to its own customers and once it was made aware of the recipient account possibly being used for scam purposes, it took the appropriate actions to prevent further transfers being made to them.

Mr M wasn't satisfied and so he complained to this service with the assistance of a representative who argued the payments were out of character and the pattern of transactions should've been seen as high risk because Mr M had never bought cryptocurrency before, so the frequent payments to a new, merchant associated with cryptocurrency should have also been seen as a change in the operation of the account.

The representative explained that Mr M recalled that some payments were blocked, but he was only asked if he'd authorised the payments. They argued that he should have been asked probing questions and had they done so they'd have realised the returns were unrealistic, the scammer had used remote access software to gain access to his device and he was sending funds to an unregulated third-party broker through a cryptocurrency exchange.

Our investigator recommended that the complaint should be upheld. She felt the third payment on 15 May 2023 for £7,210 should've raised concerns because of the value of the payment and the fact the amounts had increased in value over a few days. She explained Wise ought to have provided a tailored written warning relevant to cryptocurrency scams during the in-app chat verification process and had it done so it would have been apparent that Mr M was falling victim to a scam.

She recommended that Wise should refund the money that Mr M had lost from the third payment onwards, but she felt there were red flags which Mr M should have identified including the fact he'd been promised unrealistic returns. This should've raised concerns and lead him to carry out additional checks which he failed to do, so she thought the settlement should be reduced by 50% for contributory negligence.

Wise asked for the complaint to be reviewed by an Ombudsman. It explained that for the second and third payments, Mr M gave the payment reasons as 'sending money to friends and family' and 'sending money to yourself'. He was also shown a scam warning and after the third payment it contacted him via email in response to which Mr M said "I am transferring money to my own account with TAP. I am making this transfer in order to fund my TAP Account." When asked what TAP is, he stated: "I do have an app with name Tap. Their website is withtap.com I am using this app for card purchases and for buying crypto for myself."

It commented that payments three to five were to an account in Mr M's name which was verified by Confirmation of Payee, so it seemed he was making transfers to his own accounts. This raised no suspicions about the fraudulent nature of the transactions and the fact they were for an investment wasn't apparent until after it received the complaint.

### **My provisional findings**

I thought about whether Wise could have done more to recover the debit card payment when Mr M reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Wise) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mr M).

Mr M's own testimony supports that he used a cryptocurrency exchange to facilitate the transfer. It's only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchange would have been able to evidence it had done what was asked of it. That is, in exchange for Mr M's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I was satisfied that Wise's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

I was also satisfied Mr M 'authorised' the payments for the purposes of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although he didn't

intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, Mr M is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr M didn't intend his money to go to scammers, he 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*

Wise was an emoney/money remittance provider and at the time these events took place it wasn't subject to all the same rules, regulations and best practice that applied to banks and building societies. But it was subject to the FCA's Principles for Businesses and BCBS 2 and owed a duty of care to protect its customers against the risk of fraud and scams so far as reasonably possible.

I thought about whether Wise could have done more to prevent the scam from occurring altogether. Wise ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I needed to consider whether it ought to have intervened to warn Mr M when he 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 Mr M from financial harm due to fraud.

Mr M was shown a scam warning before the second and third payments, so I considered whether this was effective. The first payment was low-value, and so even though it was to a cryptocurrency exchange, there would have been no reason for concern. Similarly, even though the second payment was to a new payee, it wasn't identifiably linked to cryptocurrency, and it was only for £2,100, so I was satisfied a written warning was sufficient in the circumstances.

However, by the time Mr M made the third payment, even though the payment had been verified by Confirmation of Payee and he was paying an account in his own name, considering the amount and the fact Mr M had confirmed by email that he was buying cryptocurrency, I thought Wise ought to have done more.

It ought to have contacted Mr M via its in-app chat to ask him some probing questions about the payments and to provide tailored warnings about cryptocurrency scams. Had it done so, even though the payment reasons he gave weren't accurate, he went on to tell Wise he was buying cryptocurrency, so I thought he'd likely have explained that he was investing in cryptocurrency with the assistance of a broker who claimed to work for B and who had made the payments on his behalf by gaining access to his laptop using remote access software.

It's unlikely there would have been any warnings about the broker on either the Financial Conduct Authority ("FCA") or International Organisation of Securities Commissions ("IOCSO") websites, but I thought it would have been clear from the circumstances that Mr M was being scammed and Wise could have warned him there were red flags present indicating he was a victim of fraud. It could also have given him a tailored warning and provided advice on additional due diligence. And as there was no evidence that Mr M was keen to take risks, I thought he'd have followed the advice and, ultimately, decided not to make any further payments to the scam. Consequently, I was minded to direct Wise to refund the money Mr M lost from that point onwards.

### *Contributory negligence*

I accepted there's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence but, in the circumstances, I didn't think Mr M was to blame for the fact he didn't foresee the risk.

In recent years instances of individuals making large amounts of money by trading in cryptocurrency have been highly publicised to the extent that I didn't think it was unreasonable for Mr M to have believed what he was told by the broker in terms of the returns he was told were possible, notwithstanding the fact it was highly implausible.

Mr M hadn't invested in cryptocurrency before and so this was an area with which he was unfamiliar. He wouldn't have known the returns were unrealistic or how to check the information he'd been given. This unfamiliarity was compounded by the sophisticated nature of the scam, the fact he trusted the broker, he'd been introduced by a colleague and believed the trading platform was genuine and was reflecting the fact his investments were doing well.

There wouldn't have been any warnings about the broker on either the Financial Conduct Authority ("FCA") or International Organisation of Securities Commissions ("IOCSO") websites which would have alerted Mr M to the fact there was a scam. He wouldn't have known that the use of remote access software was a red flag for fraud, and I didn't consider that he went ahead in the face of any effective warnings from Wise. So, while there are instances where a reduction for contributory negligence is appropriate, I wasn't minded to conclude that this is one of them.

### *Compensation*

I thought carefully about everything that had happened, and with all the circumstances of this complaint in mind, I didn't think Wise needs to pay any compensation given that I didn't think it acted unreasonably when it was made aware of the scam. And he wasn't entitled to compensation for legal fees, as our service is free to access.

### *Recovery*

Mr M had described that he paid an account in his own name and from there the funds were moved to an online wallet in the scammer's control, so I was satisfied there was no prospect of a successful recovery.

### **Developments**

Mr M has said he is happy to accept my provisional findings and Wise hasn't provided a response.

### **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.

Because neither party has made any further comments or submitted any additional evidence for me to consider, the findings in my final decision will be the same as the findings in my provisional decision.

### **My final decision**

My final decision is that Wise Payments Limited should:

- Refund Mr M the money he lost from the third payment onwards.
- 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 Mr M with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 24 July 2024.

Carolyn Bonnell  
**Ombudsman**