DRN-4481114

The complaint

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

What happened

Mr B came into contact with someone who I'll refer to as "the scammer" who claimed to work for Company V. The scammer told him he could make money by investing in cryptocurrency. He instructed him to set up accounts with Wise and a cryptocurrency exchange company I'll refer to as "B". He also instructed him to download an 'AnyDesk' remote access software onto his mobile. Before going ahead, Mr B asked the scammer for confirmation that he was working for V and looked at to the company website, which looked professional and convincing.

The scammer told Mr B to first purchase cryptocurrency through B and then load it onto an online wallet. Between 4 August 2022 and 2 October 2022, he made seven card payments and one online transfer totalling £53,040 without any intervention from Wise. The transfer, which was for £8,000, was paid to an individual on 20 September 2022.

Mr B realised he'd been scammed when he tried to withdraw £10,000 and was asked to pay £30,800 tax on his profits. He contacted Wise to report the scam, but it refused to refund any of the money he'd lost. It said there was no spending history to compare the payments with and he'd authorised the payment. It said it was for Mr B to ensure the legitimacy of the recipient and it was unable to recall the payments because the funds went to an account of a Wise customer who was unwittingly part of the scam or a victim.

Wise said that once funds are loaded from Wise to cryptocurrency exchange companies, the service is considered provided so there was no prospect of a successful chargeback, and it was unable to recover the funds because the payments were 3DS approved and the merchant hadn't responded to its requests. It also said it had closed Mr B's account and he would need to submit an appeal so it could send it back his money to his bank account.

Mr B wasn't satisfied and so he complained to this service. He said Wise knew B was used by scammers and it should have provided an effective warning as the payments were unusual.

My provisional findings

I explained the Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, but the CRM code didn't apply to the transfer. And its most likely that B would have been able to evidence that Mr B had received the cryptocurrency, so any chargeback was destined fail. Therefore I was satisfied that Wise's decision not to raise a chargeback request was fair.

I was satisfied Mr B 'authorised' the payments for the purposes of the 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, he is presumed liable for the loss in the first instance.

I explained there's no dispute that this was as scam and that V was a clone of a genuine company. But although Mr B 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

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 B 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 B from financial harm due to fraud.

The payments didn't flag as suspicious on Wise's systems. There was no previous spending on the account to compare the payments with, and so I needed to consider whether Wise ought to have intervened based on the nature of the payments. It would have been obvious that Mr B was buying cryptocurrency and I agreed with our investigator that £10,000 is a significant amount. I also agreed that Mr B should have been given a written warning that broadly covers scams and as Wise had failed to do this, it missed an opportunity to intervene.

However, if Mr B had been presented with a written warning, while I accepted he had demonstrated some caution before choosing to go ahead with the investment, I thought he was satisfied the investment was genuine and I didn't think a written warning would have made a difference to his decision to go ahead with the payments. So, I didn't think Wise's failure to intervene when he made the first payment represented a missed opportunity to prevent the scam.

However, on 12 September 2022, Mr B made a payment of £9,900 and I thought at this point Wise should have contacted him either by phone or live-chat to ask some questions about the purpose of the payments. By this time, he had already paid £17,000 to a cryptocurrency merchant and so Wise should reasonably have asked him why he was making the payments, whether there was a third party involved and if so, how he met them, whether he'd been advised to download remote access software, whether he'd been promised unrealistic returns and whether he'd been allowed to make small withdrawals.

There's no evidence he'd had been coached to lie and so if he'd been asked these questions, I thought he'd probably have said he'd been allowed to withdraw £100 and that he'd taken advice from a broker who had told him to download AnyDesk and to make an onwards payment from the cryptocurrency exchange.

There are warnings about a company with a similar name to V on the Financial Conduct Authority ("FCA") website which might have confirmed that it was a clone of a genuine company. But even if a search of the company name didn't bring up the warning, I thought Wise would have had enough information to identify this as a scam. And if Mr B had been given a tailored warning along with clear advice on how to check the investment company was genuine, I thought he'd probably have listened to that advice and discovered he was being scammed.

Because of this, I thought Wise missed an opportunity to intervene in circumstances when to do so might have prevented Mr B's loss. Consequently, I was minded to direct it to refund the money he lost from 12 September 2022 onwards.

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence. Mr B hadn't invested in cryptocurrency before and so this was an area with which he was unfamiliar. He had explained that he checked the company website and was satisfied V was a genuine company. He also sought confirmation that the scammer worked for V and was reassured by the fact he'd been able to make a small withdrawal.

I could see from Mr B's communications with the scammer that he enquired about whether V was registered with the FCA. There's no evidence that he checked the FCA website, but I didn't think his failure to do so meant he was negligent, and I was satisfied that he did what he thought was reasonable due diligence. Therefore, whilst there may be cases where a reduction for contributory negligence is appropriate, I didn't think this was one of them.

Developments

Wise has indicated that it accepts the findings in my provisional decision.

Mr B has further argued that he made the first payment on the day he set up the account and the fact he paid in £10,000 followed by an immediate transfer out to B on the day he opened the account should have raised concerns. He believes this showed he was under pressure to make the payment and that Wise ought to have intervened.

Mr B has also questioned my conclusion about how he would have responded to a written warning. He's explained that he had no experience with cryptocurrency and had exercised due diligence before investing. He wasn't aware of the risks associated with cryptocurrency and had no reason to suspect he was being scammed. He has said that if Wise had warned him that he might be at risk, he would have sought advice from the Fraud Office and other organisations before making any further payments.

He has also commented that Wise closed his account without notice, which was an attempt to avoid responsibility for its error and to eliminate any evidence by denying him access to his account history. He has also suggested that the outcome rewards Wise for its negligence and that it should be required to refund the money he lost from 4 August 2022 onwards along with a punitive charge of either compensation or a donation to a charity of his choice.

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've considered the additional points Mr B has raised in response to my provisional decision, but I'm afraid the findings in my final decision will remain the same.

I'm aware the first payment Mr B made to the scam was on the day the account was opened and as I've previously explained, I accept it would have been obvious that he was paying a cryptocurrency merchant, and that £10,000 is a significant amount. But I maintain a written warning wouldn't have made a difference to the outcome.

Mr B has commented that this conclusion is without foundation, but it is based on the available evidence and what I think it most likely to have happened. As the account was newly created and there was no account history to compare the payment with, Wise was only required to provide a written warning which broadly covered scams. And while I accept Mr B had no experience of investing in cryptocurrency and didn't know about the scam risk, he has previously said he asked the scammer to provide proof of his status in response to which he received an official-looking email. He also searched online for V and found confirmation that it was a large international company, and he'd made a withdrawal of £100.

So, while I accept he wasn't keen to take risks, I'm satisfied the checks he'd done meant he was confident the investment was genuine to the extent that I don't think a written warning when he made the first payment would have made a difference to his decision to go ahead with that payment.

Because of this, I maintain my position that Wise should refund the money Mr B lost from 12 September 2022 onwards.

Finally, I don't think Wise needs to pay any compensation given that I don't think it acted unreasonably when it was made aware of the scam. And if Mr B wishes to pursue a complaint about the closure of Mr B's account he will have to first raise a complaint with Wise.

My final decision

My final decision is that Wise Payments Limited should:

- refund the money Mr B lost from 12 September 2022 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 B with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 20 February 2024.

Carolyn Bonnell
Ombudsman