DRN-4328296

The complaint

Ms T complains that Wise Payments Limited didn't do enough to protect her from the financial harm caused by a scam, or to help her recover the money once she'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.

Ms T received a WhatsApp message from a woman who I'll refer to as "the scammer" who claimed to work for a company I'll refer to as "W". The scammer said she had an opportunity for part time work, explaining the role involved clicking on different products to submit product data which would automatically generate a rating and recommend the products to their respective marketplace, which in turn would improve the algorithm of each product.

Ms T had uploaded her CV to different recruitment sites so it wasn't surprising that she'd been contacted. She was told she'd have to add deposits to the platform to simulate 'buying' items, and that each task would use up some of the deposit, but she would earn a commission that would be added to the account. At the end of a 'set' of 40 tasks, the employee has the opportunity to withdraw their commission as well as the original deposit that was used to 'purchase' the items.

She was told she would earn a basic salary of 1,000 USDT a week and that she would have to top up the account using cryptocurrency. The scammer asked her to purchase the cryptocurrency through a cryptocurrency exchange company and then load it onto an online wallet.

Before she put any funds in, Ms T was able to withdraw a small amount back to her cryptocurrency wallet. She reviewed the website, which looked very professional and provided ID as part of W's verification checks. She was added to a group chat with other freelancers who regularly posted about their profits. She was also told to download AnyDesk remote access software.

Between 27 January 2023 and 7 March 2023, Ms T made 39 payments to several different beneficiaries totalling £55,540. The final five payments were returned, meaning her total loss was £42,040. She realised she'd been the victim of a scam when she tried to withdraw her profits and was told she'd need to deposit an additional £53,000 on top of the money she'd already paid.

Ms T complained to Wise but it refused to refund any of the money she'd lost. It said it had attempted to recover the funds, but no funds remained apart from one payment which had been refunded. It explained that once a transfer is sent, the funds are no longer under Wise's control, the obligation of ensuring the legitimacy of the recipient lies with the sender of the payment and it is unable to be involved in disputes between senders and recipients. It also said it can't be held liable when a loss occurs as a result of fraudulent behaviour on behalf of the recipient after a payment has been made to them.

Ms T wasn't satisfied and so she complained to this service with the assistance of a representative. The representative argued that Ms T had never purchased cryptocurrency before, most of the scam payments were much larger than any of the other payments on the account and she suddenly began making large and frequent transfers in and then straight out again to multiple different new payees, which is consistent with known scam behaviour.

They said Wise should have contacted Ms T and questioned her about the payments and had it done so it would have seen the typical red flags of a task based scam including being contacted on WhatsApp and receiving small returns over the first few days. They would then have been able to warn her that she was being scammed and prevent her from making any further payments.

Wise said it couldn't have predicted that the transfers fraudulent as the payments weren't unusual for the account. They said Ms T often withdraws funds upon receipt into the account, leaving the balance empty or close to empty. She also transfers to multiple recipients and her own account.

It said Ms T was asked about the purpose of thirteen of the payments and she said she was paying friends and family, in response to which she was warned that scammers often create fake profiles online to trick people into giving them money. She was also warned that if she got a message on social media, it could be a scammer who has hacked someone's account. It accepts it could have shown additional warnings but it doesn't believe this would have changed the outcome.

Our investigator didn't think the complaint should be upheld. He was satisfied that Wise had provided warnings but as Ms T said she was paying friends and family, it was prevented from identifying that the payments were being made to a scam.

Ms T asked for the complaint to be reviewed by an Ombudsman. Her representative maintained the payments were out of character and Wise should have intervened when she sent £2,000 following a payment of £3,500 which increased the spend to £5,500 in quick succession. They argued Wise should have intervened even though she selected the wrong payment reason and as she hadn't been coached to lie, it would have uncovered the scam. They said a written warning didn't amount to a sufficient intervention and that it should have contacted her and asked questions about the payments.

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, like the one Ms T says she's fallen victim to, in all but a limited number of circumstances. But the code didn't apply to these payments because Ms T received the cryptocurrency she paid for.

I was satisfied Ms T 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although she didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of her bank account, Ms T is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Ms T didn't intend her money to go to scammers, she 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 of 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 BCOBS 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. Buying cryptocurrency is a legitimate activity and from the evidence I'd seen, the payments were made to genuine cryptocurrency sellers. However, 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 Ms T when she 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 Ms T from financial harm due to fraud.

The first payment wasn't identifiably linked to cryptocurrency and while £3,499 is significant, I didn't think it was so high that Wise needed to intervene. And while the payment reference on the second transfer did indicate a link to cryptocurrency, I didn't think the amount was so high that Wise ought to have intervened then either.

However, on 30 January 2023, Ms T transferred five payments in one day totalling £9,500. Each payment was to an individual, so it wouldn't have been apparent that she was buying cryptocurrency. But Ms T was making consecutive payments to multiple new payees having made a payment the previous day that appeared to be linked to cryptocurrency. I thought this was a pattern of spending which ought to have been concerning and so I thought Wise should have intervened when Ms T made the fifth payment that day.

Ms T was presented with a written warning before thirteen of the payments and so I considered whether this was proportionate in the circumstances. I was satisfied the warning was relevant considering Ms T had said the payment was for friends and family and that her response meant Wise was prevented from identifying that she was buying cryptocurrency, which meant it was prevented from uncovering the scam or giving a more tailored warning.

I considered whether Wise ought to have contacted Ms T either by phone or via its live chat facility and based on the volume and value of the payments she made on 30 January 2023, I thought, on balance, it probably should have done. However, based on the fact she continuously told Wise she was paying friends and family, I thought she'd have said the same thing if asked about the purpose of the payments during a human intervention. And had that happened, she'd have been presented with the same warning and the outcome would have been the same. So, even though I thought Wise should have contacted Ms T on 30 January 2023, I didn't think it would have made a difference.

I also considered whether Wise ought to have intervened in any of the later payments and because there were no instances where the payment volume or values were higher than the payments she made on 30 January 2023, I didn't think it needed to.

Compensation
I didn't find any errors or delays to Wise's investigation, so I didn't think she was entitled to any compensation.

Recovery

I didn't think there was a realistic prospect of a successful recovery because Ms T received the cryptocurrency she paid for.

Developments

Ms T's representative has responded to say she doesn't agree with my provisional findings. They agree Wise ought to have intervened on 30 January 2023 and they've explained that Ms T had misunderstood the question when she chose 'friends and family' as the payment reason as she thought she was being asked where she got the money from.

The representative has argued that Ms T has been punished for choosing an incorrect payment reason and this shouldn't be used to absolve Wise from liability, especially when there was no coaching. They've said it wasn't plausible that she was paying friends and family as she'd sent very large and frequent payments to several new payees and there was reference to cryptocurrency in the second scam payment.

The representative maintains that automated transfer pop-ups are insufficient for the amounts being sent which were out of character and high-risk and the intervention was ineffective and completely disproportionate to the inherent risk. They've argued that Wise should have gone beyond asking what the payment was for and scrutinised the answers using its knowledge of fraud types, including payments to cryptocurrency which are at an extremely elevated risk of fraud. EMI's know consumers are told to choose different payment options or given cover stories and as Ms T wasn't coached the scam would have been uncovered.

The representative has argued that if Wise had asked Ms T why she was sending the money, it would have immediately recognised she was buying cryptocurrency for the purpose of a job and that the platform didn't allow withdrawals before completion of a set number of tasks. Further, she'd been contacted via WhatsApp about the job opportunity and she'd received no formal employment documents.

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 further comments raised on Ms T's behalf but I'm afraid the findings in my final decision will remain the same as the findings in my provisional decision.

The representative has argued that Ms T shouldn't be punished for having given an incorrect payment reason, explaining that she thought she was being asked about the source of the funds. While I accept Ms T might have misunderstood what she was being asked, I don't accept it was implausible that she was paying friends and family and I can't fairly say Wise ought to have anticipated that the information it had wasn't accurate or that it should have asked further questions or provided speculative scam warnings on the off-chance this was the case.

The representative has also argued that Wise's intervention was disproportionate and that it should have scrutinised what it was being told by Ms T. As I explained in my provisional decision, I agree that by the time she made the fifth payment on 30 January 2023, Wise should have contacted her either by phone or via its live chat facility. However, as I've previously explained, based on the fact Ms T told Wise she was paying friends and family, I don't think a human intervention would have made any difference to the outcome. The representative has said Ms T wasn't coached to lie and that she was mistaken when she said she was paying friends and family, but she gave this answer thirteen times during the course of the scam and I think its more likely than not that she'd have given the same response had she been asked the same question via Wise's live chat facility.

I accept Wise is reasonably expected to ask probing questions and to use its knowledge if current fraud trends. But as Ms T wasn't paying a merchant which was identifiably linked to cryptocurrency and I consider she would likely have maintained that she was paying friends and family, other than a generic scam warning, I don't think there was much else it could reasonably have done to encourage her to disclose the real circumstances of the payments. And in those circumstances I maintain that an intervention on 30 January 2023 is unlikely to have made a difference to Ms T's decision to make the payments.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms T to accept or reject my decision before 24 May 2024.

Carolyn Bonnell
Ombudsman