DRN-4714672

The complaint

Miss H complains that Wise Payments Limited didn't do enough to protect her from the financial harm caused by a job scam, or to help her to 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.

Miss H was looking for a job and registered with a legitimate recruitment agency. The following morning, she received a WhatsApp message from someone who I'll refer to as "the scammer" who claimed to work for a recruitment company, which I'll refer to as "P". The scammer told Miss H about an opportunity to work remotely for an online marketing platform which I'll refer to as "A". She would be required to purchase tasks from the platform using cryptocurrency and would earn a commission from each task.

On 9 August 2023, Miss H was contacted on WhatsApp by someone who said she would be her supervisor. The supervisor said she would help her with the investment process and gave her login credentials for the account she had created for her. She also added her to a WhatsApp group of over 20 individuals who claimed to be doing the same role.

Around 13 August 2023 the supervisor told Miss H to open a Wise account because it would be an easier way to send the funds required to purchase each task. The supervisor told her to send funds from Bank L and not to tell Bank L that she intended to buy cryptocurrency. She was then instructed to purchase cryptocurrency through cryptocurrency exchange companies which I'll refer to as "M" and "S" and then load it onto an online wallet.

Before she made any payments from Wise, she successfully made two withdrawals from the platform and between 13 August 2023 and 5 August 2023, she made thirteen payments totalling £16,150 using a debit card connected to the Wise account.

During the scam period, Miss H felt under pressure to complete more tasks to avoid losing her money, so she took out loans for £3,000, £300, and £400, telling the loan companies the loans were for debt consolidation, a vet bill, and a utility bill. The loan funds were paid into an account Miss H held with an electronic money institution ("EMI") which I'll refer to as "R" before being transferred to Wise.

On 25 August 2023, Miss H attempted to withdraw her deposits and commissions but she was told by the supervisor that the transaction had been blocked due to its size, at which point she realised he'd been scammed.

She complained to Wise, but it refused to refund any of the money she'd lost. It said card payments to investment or gambling accounts are generally considered to be completed once the funds are loaded to the account and the service was provided and so there were no chargeback rights against the cryptocurrency merchants. It said its attempts to recall the funds were unsuccessful because the merchants didn't respond to its requests. And the

transactions were 3DS approved meaning she had approved them via an SMS code, or a push notification issued to the registered device.

Finally, it apologised for the time it had taken to respond to the complaint and offered £50 compensation for delays and inconvenience.

Miss H wasn't satisfied and so she complained to this service with the assistance of a representative. She accepted she'd authorised the transactions, but she argued that Wise should have intervened because she was making substantial payments to a new payee which was a cryptocurrency merchant. She said she wanted it to refund the money she'd lost plus £250 compensation for failings in the service he'd received, and legal costs.

Her representative said Wise should have intervened because this was a new account which was opened for the purpose of the scam. Miss H made 14 payments to a new payee linked to cryptocurrency totalling £18,950. They said it should have flagged the payments and questioned Miss H, and as she wasn't prompted to give false answers, she would have disclosed that she was acting under the instructions of a supervisor. Wise should then have realised she was falling victim to an elaborate scam because there were red flags present including the fact she'd opened a new account before making payments to a cryptocurrency merchant.

Wise said as its not Miss H's primary bank, it doesn't have access to her income or savings information, so it didn't have a full understanding of her spending habits and transaction history. And the transfers weren't unusual compared to the typical use of accounts Wise.

Our investigator didn't think the complaint should be upheld. He explained Miss H was making payments from a new account so there was no account history, and the loan funds weren't initially sent to Wise, so it wouldn't have known the money was borrowed. But even if it had intervened, he didn't think Miss H would have told the truth about the payments because there was evidence she'd been coached to lie and she'd lied about the purpose of the loan applications, so she didn't think it would have uncovered the scam.

Finally, he was satisfied Wise had attempted to recover the funds and that there was no prospect of a successful chargeback because the cryptocurrency exchange companies had provided the service she paid for.

Miss H has asked for her complaint to be reviewed by an Ombudsman arguing that if Wise had warned her about job scams, she'd have realised she was being scammed. Her representative said Wise's fraud prevention systems failed to detect the unusual activity on her account and the pattern of spending meant the transactions were high-risk.

They said Wise should have asked her probing questions and even though she wasn't forthcoming with the reasons for the loans, she did this under the instruction of the scammer with a view to quickly accessing funds.

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 reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Miss H has been the victim of a cruel scam. I know she feels strongly about this complaint, and this will come as a disappointment to her, so I'll explain why.

I've thought about whether Wise could have done more to recover Miss H's payments when she 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.

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

I'm satisfied Miss H '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, Miss H is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Miss H 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 is an EMI 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've 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've seen, the payments were made to genuine cryptocurrency exchange companies. However, Wise ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have intervened to warn Miss H 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 Miss H from financial harm due to fraud.

The payments didn't flag as suspicious on Wise's systems. This was a newly opened account and so there was no account history to compare the payments with. Miss H was also paying legitimate cryptocurrency merchants and there would have been no indication that she was using loan funds, because the funds were paid into the account from R. However, the cumulative total on 13 August 2023 was £4,750 and on 15 August 2023 it was £6,100, and as these were significant amounts to a cryptocurrency merchant from a new account, I think Wise should have intervened.

We would expect Wise to have presented Miss H with a written warning asking her to answer a series of automated questions aimed at identifying the scam risk. But I agree with

our investigator that as Miss H had been coached to lie (the supervisor told her to send funds from Bank L and not to tell Bank L that she intended to buy cryptocurrency) and she had in fact lied to all three loan companies about the purpose of the loans, it's unlikely she'd have answered the questions honestly and so Wise wouldn't have detected the scam. I understand she was driven to lie to the loan companies by the need to quickly access funds to avoid losing her money, but I consider she was similarly motivated to purchase tasks in the early stages of the scam and that she trusted the scammer to the extent that she was prepared lie to her bank.

Consequently, I agree with our investigator that there was nothing Wise could reasonably have done to prevent Miss H's loss.

Compensation

The main cause for the upset was the scammer who persuaded Miss H to part with her funds. Wise has offered to pay her £50 for service issues and having considered the impact of those failings I'm satisfied that's fair.

Recovery

I don't think there was a realistic prospect of a successful recovery because Miss H paid an account in her own name and moved the funds onwards from there.

I'm sorry to hear Miss H has lost money and the effect this has had on her. But for the reasons I've explained, I don't think Wise could have prevented her loss and so I can't fairly tell it to do anything further to resolve this complaint.

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 Miss H to accept or reject my decision before 26 July 2024.

Carolyn Bonnell
Ombudsman