DRN-4517183

The complaint

Mrs B complains that UAB ZEN.COM didn't do enough to protect her from the financial harm caused by an investment 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.

Mrs B came across an investment opportunity while she was on social media. She registered her interest and was contacted by someone I'll refer to as "the scammer" who said they were a broker working for a company I'll refer to as "C". The scammer said he could help Mrs B to invest in forex and commodities and that she could earn 40% per year on her investment.

Mrs B was impressed because the scammer seemed knowledgeable and professional and was able to answer all her queries. He told her C was registered in the UK, regulated by the Financial Conduct Authority ("FCA"), and registered on Companies House.

The scammer told Mrs B to download AnyDesk remote access software to her device to facilitate the onboarding and to open an account with Zen so she could make international payments. He also gave her login details to enable her to open an account with C and told her to open an account with a cryptocurrency exchange company which she could see was a legitimate platform.

The scammer told Mrs B to first purchase cryptocurrency from individuals through a cryptocurrency exchange company and then load the cryptocurrency onto an online wallet. On 27 March 2023, she received a transfer into the account for $11,934 and on 28 March 2023, she made two transfers to international accounts for $10,990 and $928. Both payments made with no intervention from Zen.

Mrs B could see the deposits she'd made on the online platform and she could see "live" trades and returns on her investments on the trading platform. But she realised she'd been scammed on 9 June 2023 when she was told she would have to pay fees to make a withdrawal and she realised that C was a clone of a legitimate company.

Mrs B complained to Zen but it refused to refund any of the money she'd lost. It said the funds were used to buy cryptocurrency at a separate third-party platform so it couldn't have known she was buying cryptocurrency.
Mrs B complained to this service with the assistance of a representative who explained the Zen account was opened as part of the scam, so there was no transaction history to compare the payments with. They said Mrs B had deposited funds into the account before paying it out to a cryptocurrency exchange, which should have indicated she was being scammed.

They said Zen should have identified the payments as suspicious and intervened to ask probing questions, in response to which Mrs B would have told it she'd discovered the opportunity on social media and that she was told by a broker to use AnyDesk. With this information, Zen would have recognised that she was being scammed and that the investment company was impersonating a legitimate firm and wasn't registered to trade in the UK.

In further submissions to the service, Zen said it blocked a payment into the account because it was for a large amount. It asked Mrs B about the purpose of the transfer and she said it was for daily expenses and didn't mention investments.

Our investigator has recommended that the complaint should be upheld. He explained the payments couldn't be recovered as they were for legitimate P2P cryptocurrency purchases and Mrs B had received the cryptocurrency she paid for. He noted Zen carried out some enquiries with the beneficiaries and he didn't think it could have done anything more to recover the funds because she had received the cryptocurrency she paid for. He also explained the payments weren't covered under the Contingent Reimbursement Model (CRM) code because Mrs B received the cryptocurrency, Zen isn't signed up to the Code and the payments were to accounts outside of the UK.

However, he thought the payment of $10,990 Mrs B made on 28 March 2023 ought to have flagged as unusual because it was a large amount of money for a first-time transaction and was made a day after Mrs B had transferred funds into her account.

He explained that Zen should have blocked the payment, and questioned Mrs B about the payment to satisfy itself that she wasn't being scammed. He said there was no evidence she had been coached to lie so she would have told it that she was being assisted by a broker who had told her to download AnyDesk and to open the Zen account. She should then have been given a tailored scam warning, which he thought would have stopped her from going ahead with the payment.

However, he didn't think Mrs B had done enough to mitigate her loss because she went ahead with the investment having only looked at C's website. He said the scammer had sent her a link to the FCA website and if she'd checked the register, she would have realised it wasn't authorised to provide financial services in the UK. So, he thought the settlement should be reduced by 50% for contributory negligence.

Mrs B has indicated that she'd happy to accept our investigator's view, but Zen has asked for the complaint to be reviewed by an Ombudsman. It maintains the transactions from Mrs B's Zen account weren't scam payments as she received the cryptocurrency she paid for.

It accepts she was the victim of an investment scam but as she wasn't paying a cryptocurrency exchange it had no indication that she was paying P2P traders. It said it had stopped an incoming transaction to ascertain the source of funds and when it asked her the purpose of the funds, she confirmed it was for day to day usage. This concealed her intention to use the funds for an investment and it doesn't accept she would have told it about C's involvement if it had contacted her when she made the disputed transaction.

Finally, it has argued that Mrs B didn't do enough to check C was a genuine company as she should have contacted it directly or looked at the website, because the genuine company had warnings which might have alerted her to the fact she was being scammed. She invested a large sum of money without seeking independent advice and she should have been concerned that she'd found in opportunity on social media and that she was being promised returns that were above average.

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.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mrs B says she's fallen victim to, in all but a limited number of circumstances. But the CRM code didn't apply in this case because Mrs B was paying an international account, she received the cryptocurrency she paid for and Zen isn't signed up to the code.

I'm satisfied Mrs B '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, she is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mrs B didn't intend her money to go to scammers, she did authorise the disputed payments. Zen 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

Zen is an Electronic Money Institution ("EMI") and at the time the payment 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 Zen 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 sellers. However, Zen 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 Mrs B when she tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Zen to intervene with a view to protecting Mrs B from financial harm due to fraud.

The payments didn't flag as suspicious on Zen's systems. Because this was a newly opened account, there was no historic spending to compare the payments with. And its right that because Mrs B was making P2P cryptocurrency purchases, so Zen wouldn't have known she was buying cryptocurrency. However, Mrs B had received a large payment into the account followed by a very large transfer out of the account the following day and because this was the very first payment out of the account, I agree with our investigator that Zen should have contacted her to ask some questions about the purpose of the payment.

Zen has argued that it contacted Mrs B when she had received a payment into the account and that she told it the funds were for day to day usage. But it has stated that this occurred on 15 May 2023, so I don't think the interaction is relevant to the issue of whether she'd have been honest with it if it had contacted her to ask her about the payment on 28 March 2023. And in any even I don't accept that Mrs B responses to questions around payments into her

account are necessarily indicative of how she would respond to questions about payments out of the account.

Because of this, I think it's more likely than not that if she was asked questions about the payments, she'd have said she was buying cryptocurrency on the advice of a broker she'd found on social media. I think she'd have also told it the broker had told her to open the Zen account and to download AnyDesk to her device.

With this information, Zen would have been able to identify that she was being scammed and it could have told her there were red flags present that the investment was probably a scam. It would have also told her how to check the investment was genuine including how to check the FCA register.

I haven't seen any evidence that Mrs B was keen to take risks and so I'm satisfied she'd have listened to Zen's advice and decided not to go ahead with the payment. Because of this I'm satisfied that it missed an opportunity to intervene in circumstances which might have prevented her loss and so it should refund the money she lost.

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence. While I accept this was a sophisticated scam, I'm satisfied Mrs B was made aware of the existence of the FCA and that she failed to conduct checks that might have uncovered the scam sooner, including checking C's website, which included warnings that it was being used in scam involving cryptocurrency.

Because of this, I agree with our investigator that the settlement should be reduced by 50% for contributory negligence.

My final decision

My final decision is that UAB ZEN.COM should:

- refund the money Mrs B has lost.
- this settlement should be reduced by 50% to reflect contributory negligence.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If UAB ZEN.COM deducts tax in relation to the interest element of this award it should provide Mrs B with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs B to accept or reject my decision before 28 January 2024.

Carolyn Bonnell
Ombudsman