DRN-4290069

The complaint

Miss W complains that Wise Payments Limited didn't do enough to protect her from the financial harm caused by an investment scam company, 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.

In June 2022 Miss W saw that a friend had shared a link on social media regarding an opportunity to invest in cryptocurrency. She had seen cryptocurrency endorsed in the media by well-known celebrities and assumed the opportunity would have been vetted by the social media platform.

Miss W clicked on the link which took her to a website for a company I'll refer to as "V" which traded in Forex exchange, commodities, and cryptocurrencies. She didn't see any negative reviews or other information to raise concerns, so she completed the online enquiry form before receiving a call from someone claiming to be a financial advisor. The advisor explained she had several years of experience and that V was authorised by the Financial Conduct Authority ("FCA").

The advisor said she could help Miss W to achieve her goal and explained all traders begin with a minimum investment of £200. Miss W could hear background noise which sounded like a call centre and the advisor gave detailed and thorough responses to all her questions. She explained Miss W would have to go through KYC and Anti-Money Laundering (AML) checks, so she submitted two forms of a photo ID and proof of address.

The advisor told Miss W to open a trading account with V and an account with Wise. She also told her to download Anydesk remote access software to her device. She told Miss W she would have to transfer funds to Wise from her other bank account and then purchase cryptocurrency through a cryptocurrency exchange company before loading it onto an online wallet. Between 4 August 2022 and 18 August 2022, Miss W made three card payments and six transfers from her Wise account totalling £41,180.

Miss W could see her profits on the trading platform but when she tried to make a withdrawal, she received an email purporting to be from Wise explaining that if she wanted to liquidate her account, she would have to pay more money into her wallet. The broker explained that her money was being held by the FCA, so she agreed to make a further payment of £9,700. She was then told there had been an issue with the payment, so she had to re-send the same amount the following day.

Miss W realised she'd been scammed on 18 August 2022 when she was locked out of her trading account. She complained to Wise and it deactivated the account but it refused to refund any of the money she'd lost. It said it took appropriate action to prevent further payments once it was made aware of the recipient account possibly being used for scam

purposes, but the payments weren't flagged by its fraud systems, so it wasn't possible to detect the payments as potentially problematic.

It said the payments Miss W made on 18 August 2022 was rejected and returned, but card payments to investment accounts are generally considered complete once the funds are loaded to the account, so there were no chargeback rights. It also said the payments were 3DS approved and by installing AnyDesk and allowing the broker to access her Wise account, she failed to keep her account safe.

Miss W wasn't satisfied and so she complained to this service with the assistance of a representative who said Miss W wasn't satisfied with the £9,100 Wise had recovered. She argued that if it had intervened, she'd have explained she was investing in cryptocurrency and the scam would have been detected sooner.

Her representative has argued that Wise should have intervened when Miss W made the first payment on 9 August 2022 because it was to an international payee and resulted in a currency conversion fee, which should have been a red flag. They said the payment was out of character with the normal spending on the account due to its value and the fact the recipient was a new payee. They accepted there was a payment for £15,000 on 4 July 2022, but this was to a regular payee and between 9 April 2022 and 9 May 2022, the largest transaction on the account was £800.

The representative said that if Wise had intervened on 9 August 2022, Miss W hadn't been instructed to lie at this point, so the scam could have been avoided. They said it should have asked her why she was sending funds to another account in her own name and as she wouldn't have been prepared to think on the spot, she'd have admitted the truth and so it could have detected the scam.

Our investigator thought the complaint should be upheld. She explained there was no account history to compare the transactions with, and she didn't think the first seven payments were suspicious. But Miss W had paid £9,700 into the account on 15 August 2022, which she transferred out to a new payee within minutes. She noted this was a significant amount and Wise should've given a written scam warning. But she didn't think this would have made a difference because Miss W had believed the investment was genuine.

On 15 August 2022, a further £9,700 was credited into the account and transferred out within four minutes to a different payee. Our investigator noted the cumulative spend for the day was £19,400 within two hours, and the payment wasn't consistent with the reason given when the account was opened. So, she thought Wise should've intervened to query the nature of the payment and to provide a tailored warning.

Our investigator noted that the broker had told Miss W to lie to her other bank, but she hadn't been told to give the same cover story to Wise and if she'd told it she'd come across the opportunity on social media, it would have recognised the investment was a scam. It could then have given an effective and tailored warning and prevented the scam.

Our investigator noted the other bank had warned Miss W about scams and that if she'd done some research, she might have found the FCA warning about V dated in April 2021. Because of this, she thought the settlement should be reduced by 25% for contributory negligence.

Finally, our investigator explained that Wise had recovered £9,100 on 17 March 2023 but the funds weren't returned until after Miss W complained to this service, so she recommended it should pay interest on the amount.

Both parties have asked for the complaint to be reviewed by an Ombudsman. Wise has responded to say the settlement should be reduced by 50% for contributory negligence and Miss W has said it's not fair that Wise didn't tell her about the £9,100 that was returned to the account.

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 decided to uphold Miss W's complaint.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Miss W 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 Miss W received the cryptocurrency she paid for. And the payments to individuals were international payments.

I've also thought about whether Wise could have done more to recover the card 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 W).

Its 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 they'd done what was asked of them. That is, in exchange for Miss W'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 the cryptocurrency exchange company was fair.

I'm satisfied Miss W '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 Miss W 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

I've thought about whether Wise could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity, 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 W 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 W from financial harm due to fraud.

The payments didn't flag as suspicious on Wise's systems. I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Miss W normally ran her account and I agree with our investigator that Wise ought to have intervened on 15 August 2022 when Miss W received £9,700 into the account and transferred the same amount out of the account nine minutes later. However, as this was a new account and there was no spending history to compare the payment with, it only needed to provide a written warning and I agree with our investigator that a written warning wouldn't have made a difference because Miss W was convinced the investment was genuine.

Less than two hours later, Miss W made another payment of £9,700, having transferred the same amount into the account four minutes earlier. At this point, because she had paid out £19,400 in under two hours having received the same amount into the account immediately before each payment, even though it wasn't obvious that she was buying cryptocurrency, I think Wise ought to have contacted Miss W either by phone or live-chat and asked her why she was making the payment.

When Miss W was contacted by her other bank on 17 August 2022, she told it she was sending money to a friend who lived abroad, having been advised to lie by the scammer because the bank didn't allow payments to cryptocurrency exchanges. This raises concerns that Miss W might have provided the same cover story to Wise had it intervened. However, she has explained that she wasn't told to give the same cover story to Wise as she believed she was sending funds from her Wise account to her cryptocurrency account through person to person verification, which was needed to prove she held funds in her Wise account.

Miss W has produced an email from Wise dated 16 August 2022 which she later learned was part of the scam, which supports that she believed she was sending funds from her Wise account for verification purposes and, based on this evidence and the explanation she has given about why she thought she was sending money from her Wise account, I'm satisfied, on balance, that she would have answered truthfully if Wise had asked her about the purpose of the payment.

With this in mind, I would expect Wise to have asked Miss W why she was making the payments, whether there was a third party involved and if so how she met the third party, whether she'd been told to download remote access software, whether she'd been promised unrealistic returns and whether she'd been told to make an onwards payment from the cryptocurrency exchange. And as I've accepted Miss W would have been honest in her responses, I'm satisfied she would have told Wise that she was taking advice from someone who worked for company V, which she'd learned about on social media. I think she would have also told the call handler that she'd been advised to download AnyDesk and to transfer the cryptocurrency into a wallet provided to her by the scammer.

With this information, I'm satisfied there were enough red flags present for the call handler to have identified that the investment was a scam and I would expect her to have been given a tailored warning including advice about clone companies. I would also expect the call handler to have discussed with Miss W the nature of the checks she'd undertaken and to have provided advice on additional due diligence, including how to contact the details on the FCA website to check V was a genuine company.

When Miss W spoke to her other bank on 17 August 2022, she was told that being asked to lie would be an indication that the investment was probably a scam. I accept that she continued to make payments to the scam because she thought the cover story was necessary because the bank wouldn't allow payments to cryptocurrency. And I'm satisfied that if Wise had brought to her attention the fact that there were red flags present which indicated that the investment was probably a scam, she would thought twice about what she

was being asked to do and conducted further checks, which would have uncovered the fact that V was a clone of a genuine company.

Because of this, I'm satisfied that Wise missed an opportunity to intervene and that this represented a missed opportunity to have prevented Miss W's loss.

Contributory negligence

Our investigator recommended that the settlement should be reduced by 25% for contributory negligence.

I've considered the circumstances leading up to the point when Miss W made the second payment on 15 August 2022, and I don't think it was unreasonable for her to have believed what she was told by the scammer.

She has described that her friend had shared a link on social media and she had assumed the link would have been vetted by the social media platform. She has also explained that she didn't see any negative reviews and she had heard what she thought sounded like a call centre in the background when she spoke to the scammer. She was also reassured by the fact she'd been required to compete AML checks and provide photographic ID. And I've seen evidence of the documents she received from the scam, so I'm satisfied the scam was sophisticated. Miss W hadn't invested in cryptocurrency before and this was an area with which she was unfamiliar, so she wouldn't have known to check with the FCA before going ahead with the investment. This unfamiliarity was compounded by the sophisticated nature of the scam and the fact she trusted the scammer and believed the trading platform was genuine. Because of this, I don't agree that the settlement in respect of this payment should be reduced for contributory negligence.

However, by the time Miss W made the final payments on 17 August 2022, she had been told by the scammer to lie to her other bank. And she went ahead with those payments having been warned that being told to lie would be an indication that the investment was a scam. Because of this, I'm satisfied that the settlement in respect of the payment she made on 17 August 2022 should be reduced by 50% for contributory negligence.

Recovery

Wise recovered £9,100 on 17 March 2023, but the funds weren't returned to Miss W immediately. Because of this I agree with our investigator that it should pay interest on the amount from the date it recovered the funds to the date the date the funds were returned to Miss W.

F**inal decision**

My final decision is that Wise Payments Limited should:

- Refund the payments Miss W made from the second payment on 15 August 2022 (less the £9,100 it recovered).
- The part of the settlement which relates to the payment Miss W made on 17 August 2022 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.
- It should also pay 8% simple interest on the £9,100 recovered from the date it first recovered the funds until the date the money was returned to Miss W.

*If Wise Payments Limited deducts tax in relation to the interest element of this award it should provide Miss W with the appropriate tax deduction certificate.

My final decision

Your text here

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss W to accept or reject my decision before 26 January 2024.

Carolyn Bonnell
Ombudsman