DRN-4360505

The complaint

Miss F complains that Revolut Ltd 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.

In 2022, Miss F saw some advertisements relating to cryptocurrency investments, which she didn't pursue because she didn't have any knowledge or experience of investing. However, in May 2022, a close friend told her she'd been investing in cryptocurrency with an investment company I'll refer to as "S". The friend showed Miss F her trading account showing profits over £10,000 and encouraged her to look more closely at the opportunity.

She followed a link provided by her friend and was directed to S's website which included an about us section, FAQs, and a 24/7 live chat option. It also provided full details of the company directors, giving a brief synopsis of their experience and confirmed its traders could access currency pairs, stocks, and nine different cryptocurrencies.

Miss F checked Trust Pilot and Yell noting S had received four-star reviews, and there were several testimonials from previous clients. She completed an online enquiry form and shortly afterwards she received a call from someone I'll refer to as the scammer who claimed to work for S. He said he had a background in finance and that she'd be given an online trading account and an investment broker to advise on how and what to invest in. He gave detailed and thorough responses to all questions and after several long conversations Miss F decided she wanted to invest.

The scammer told her to open a trading account which required her to provide two forms of photo ID as part of the KYC and Anti-Money Laundering (AML) regulations. He also told her to download AnyDesk remote access software explaining it would allow him to trade on her behalf and guide her through the process. When Miss F logged into the trading portal she noted it showed the fluctuating exchange rates of various currencies. The scammer said there was no minimum deposit but the higher the deposit the more likely Miss F would be to reach higher profits. He also said she could expect a 25% return on her investment.

On the advice of the scammer, Miss F opened an account with a cryptocurrency exchange company I'll refer to as "C". She also opened an account with Revolut and funded it with credits of £2000 and £3000. The scammer asked her to first purchase cryptocurrency through C and then load it onto an online wallet, and on 3 June 2022 she paid £4,920.02 to C using a Visa debit card connected to her Revolut account.

Miss F watched as her profits increased, and the scammer gave her constant updates. But when she said she wanted to make a withdrawal she was met with resistance and told to pay a series of fees. The scammer grew increasingly aggressive and confrontational

suggesting she could lose everything if she didn't pay the fees, at which point she realised she'd been scammed.

Miss F complained to this service with the assistance of a representative. She said Revolut was very dismissive when she reported the scam and she doesn't think she received an acceptable level of customer service. The representative said Revolut had failed to raise a chargeback request. They also argued that Miss F had opened the account and funded it with several high value credits before making an unusually high payment to a new payee associated with cryptocurrency. Such a rapid withdrawal from a new account should have been alarming and so Revolut should have intervened.

The representative said it ought to have contacted Miss F and asked her what the payment was for and whether there were any third parties involved. It should have asked what returns she'd been promised and how the broker got her details. Had it done so as she hadn't been coached to lie, she'd have said she was being assisted by a broker and the scam would have been prevented.

Responding to the complaint, Revolut commented Miss F was out of time to raise a chargeback dispute and that C had provided the service in full and service was as described. It said it had no reason to stop the payment or provide a warning because the funds were transferred to an account in Miss F's own name and the payment was 3DS authenticated, so it couldn't have been completed without her permission. It said the account was opened on 31 May 2022, and there was no other activity on the account prior to the transaction which it could have used to determine unusual activity. And the payment wasn't made directly to S.

Finally, it also argued that Miss F failed to conduct reasonable due diligence explaining that a simple google of the scam company would fetch results indicating it was a scam.
Our investigator didn't think the complaint should be upheld. She didn't think the payment was particularly unusual or suspicious because it wasn't high value and there wasn't a pattern of payments which would indicate fraud. She also said C was a legitimate cryptocurrency exchange and Miss F was paying an account in her own name, so she didn't think it missed an opportunity to intervene. Further, she didn't speak to or interact with Revolut at the time of the payment, so it didn't miss an opportunity to identify the payments were being made in relation to a scam.

She also commented that even if Revolut had sent a tailored warning, this would have been sent after the payment was made and was there was only one payment, it wouldn't have impacted any future loss.

Finally, our investigator explained the chargeback rules don't cover scams and we would only expect Revolut to raise a chargeback if it was likely to be successful. She explained Miss F had paid a legitimate cryptocurrency exchange which would be able to show she received a service, so there wasn't a reasonable prospect of a successful chargeback.

Miss F has asked for her complaint to be reviewed by an Ombudsman. Her representative has argued that Miss F hadn't invested before and the payment was high enough for Revolut to have intervened, especially as newly opened accounts present a greater risk of misuse. They maintain this was a high value, one off payment to a cryptocurrency platform from a newly opened account and Miss F wouldn't have gone ahead if she'd been provided scam education.

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 F 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 Revolut could have done more to recover Miss F's payment when she reported the scam to it. Chargeback is a voluntary scheme 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 the arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Revolut) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Miss F).

Miss F's own testimony supports that she used a cryptocurrency exchange to facilitate the transfer. 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 F's payment, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Revolut's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

I'm also satisfied Miss F 'authorised' the payment 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 F didn't intend her money to go to scammers, she did authorise the disputed payments. Revolut 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

Revolut 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've thought about whether Revolut 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 payment was made to a genuine cryptocurrency exchange company. However, Revolut ought to fairly and reasonably be alert to fraud and scams and this payment was part of a wider scam, so I need to consider whether it ought to have intervened to warn Miss F when she tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Revolut to intervene with a view to protecting Miss F from financial harm due to fraud.

This was a newly opened account and so there was no account history to compare the payment with. I accept Miss F made two large credits into the account before paying out £4,920.02 to C on the day she opened the account and I also note the representative's

comments regarding the risks associate with newly opened accounts. But the payment was 3DS authenticated, she was paying an account in her own name with a legitimate cryptocurrency exchange and I don't think the payment was so high that Revolut needed to intervene.

Further, if Revolut's fraud systems had triggered, based on the size of the payment, I think a written warning which broadly covered scams would have been proportionate to the risk, and would likely have been presented after the payment was processed, so it wouldn't have prevented her loss. And even if a warning was shown before the payment was processed, this investment was recommended by a friend who had shown her profits on her trading account, so she had no reason to suspect it wasn't genuine. And I'm satisfied Miss F was convinced the investment was genuine to the extent that a written warning wouldn't have made any difference to her decision to go ahead with the payment, so I don't think Revolut missed an opportunity to prevent her loss.

Compensation

The main cause for the upset was the scammer who persuaded Miss F to part with her funds. I haven't found any errors or delays to Revolut's investigation, so she's not entitled to any compensation or legal costs.

Recovery

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

I'm sorry to hear Miss F has lost money and the effect this has had on her. But for the reasons I've explained, I don't think Revolut is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

My final decision

For the reasons I've outlined above, 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 F to accept or reject my decision before 30 April 2024.

Carolyn Bonnell
Ombudsman