DRN-5386284

The complaint

Ms M 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 February 2023, Ms M saw an advert on social media for an investment opportunity with a company I'll refer to as "J", which was endorsed by a well-known celebrity. Ms M completed an online contact form and received a call from someone I'll refer to as "the scammer" who said he was a broker. Unfortunately, J was in fact a clone of a genuine company which was regulated by the Cyprus Securities and Exchange Commission (CySEC), and which had 'passporting' rights through the Financial Conduct Authority (FCA) – which meant it could offer its services to UK customers as recorded on FCA website.

The scammer asked Ms M to send proof of ID and to download 'AnyDesk' remote access software so he could help her to trade. He asked her to first purchase cryptocurrency through a cryptocurrency exchange company ("B") and then load it onto an online wallet. Ms M topped up her Revolut account with funds from Bank S, and on 6 February 2023 and 17 February 2023, she made seven card payments to "B" totalling £22,900.

Ms M could see her profits on her trading account, and when her balance reached £53,000, she asked to withdraw £10,000, and was told she'd have to pay more funds into the account. When she told the scammer she couldn't afford to do so, the scammer said that if she put in £4,000, he would match it. At this point, she spoke to a friend who alerted her to the scam.

Ms M complained to Revolut with the assistance of a representative who said Revolut should have intervened because she was sending funds to a new payee linked to cryptocurrency, which was unusual for the account. They explained Ms M mainly uses the account to send money to her family and friends abroad and the highest payment on the account was £2,700, so the payments were unusual. They said it should have asked why she was making the payments, whether there was a third party involved, how she found out about J, whether she'd done any research, whether she'd been promised unrealistic returns and whether she'd received any withdrawals. And as she hadn't been prompted to give false answers, it would have been apparent that she was falling victim to a scam.

But Revolut refused to refund any of the money she'd lost. It said Ms M's chargeback claims had been rejected because the payments were money orders, and the service was considered "provided as described'. It also said the payments were authenticated via its 3DS authentication system, so the claims weren't valid under the card scheme rules.

Ms M wasn't satisfied and so she complained to this service. She said she'd never invested before and had acted in good faith believing the investment was genuine. She also said the

payments were unusual for her account and Revolut missed multiple opportunities to stop the payments.

Revolut further argued that the payments were made to accounts with cryptocurrency exchanges in Ms M's control, so the fraudulent activity didn't occur via the Revolut platform. t said it was used as an intermediary to receive funds from Ms M's main bank account and she lost control of the funds further in the chain. It said the transactions weren't out of character for the account and there was a gap of eleven days between the first and second payments, so she had sufficient time to perform due diligence and there was no indication that she was acting under duress.

Our investigator didn't think the complaint should be upheld. She commented that the first payment was low value and so Revolut didn't need to intervene, but it should have intervened on 17 February 2023 when Ms M paid £5,000 to B (the second payment) because it was a large payment to a high-risk cryptocurrency merchant. She said it would have known the payment was going to a cryptocurrency merchant and so she'd expect it to have provided a tailored written warning relevant to cryptocurrency investment scams covering off key features of the scam.

But she didn't think a this would have made a difference because the evidence of Ms M's interactions with the scammer suggested she had full trust in the investment. She'd received some credits which would've added her impression that this was a genuine investment and had been given a letter of guarantee which included the 'terms of agreement' and details of her trading account and ID.

Our investigator explained that as J was a clone of an FCA regulated company with the same name, any research would have likely brought her to the genuine company's website. So, while she thought Revolut did miss an opportunity to intervene, she didn't think this represented a missed opportunity to prevent the scam.

Finally, our investigator explained that even it Revolut taken steps to recover Ms M's funds, it wouldn't have made a difference because she'd transferred funds to an account in her own name before moving them onwards to the scam. And any chargeback claim would have been unsuccessful because a service was provided by the cryptocurrency exchange.

Ms M asked for her complaint to be reviewed by an Ombudsman arguing that Revolut failed to provide adequate warnings about the risk of fraud which could have alerted her to the scam and prevented her loss.

Her representative reiterated that Revolut should have asked Ms M whether someone was asking her to make the payments, how she learned about the investment and whether she was being pressured or rushed to make the payment. And they dispute that she'd have continued with the payments following a written warning from Revolut arguing it has a responsibility to provide clear warnings and its failure to do so represented a failure to protect her from foreseeable harm.

My provisional findings

I issued a provisional decision on 12 February 2025, in which I stated as follows:

I'm satisfied Ms M '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 M is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Ms M 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

In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

But, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in February 2023 that Revolut should:

• have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;

• have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;

• in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment;

• have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi- stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

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 payments were made to a genuine cryptocurrency exchange company. However, Revolut 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 Ms M 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 Ms M from financial harm due to fraud.

The payments didn't flag as suspicious on Revolut's systems. I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Ms M normally ran her account, and I think they were. The first payment was for £200, and so even though Ms M was paying a cryptocurrency exchange, Revolut wouldn't have needed to intervene. However, when she made the second payment on 17 February 2023, even though the transfers didn't contradict the account opening purpose, I would expect it to have intervened because she was sending £5,000 to a high-risk cryptocurrency merchant.

I think a proportionate response would have been to provide a written warning covering some of the key features of cryptocurrency-related investment scams, including the fact

victims are usually targeted via social media and that scammers often utilise fake celebrity endorsements and encourage the use of remote access software.

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case and on the balance of probabilities, I don't think it would have. There were several key hallmarks of common cryptocurrency investment scams present and so I think the warning might have resonated with Ms M, and I haven't seen any evidence that she was asked, or agreed to, disregard any warning provided by Revolut.

However, while I have no reason to think she wouldn't have paused and looked more closely into the circumstances of the investment before proceeding, as J was a clone of a genuine company, a basic search would likely have shown information which would have satisfied Ms M that the investment was genuine. And this, along with the documentation she'd received from the scammer and the fact she'd successfully withdrawn £290.12 on 6 February 2023 would been enough to satisfy her that the investment was genuine. So, I don't think a written warning would have been impactful enough to have stopped her from going ahead with the payment.

Significantly, Ms M went on to make four more payments to B that day. And not only were they made in very quick succession (the final three payments happened in three minutes), by the time she made the final payment, the cumulative total was £22,700. In the circumstances I think Revolut ought to have intervened again when she made the third payment that day, and because the cumulative total for the day was £14,900, I think it should have gone further than a written warning and engaged with her via its live-chat facility.

I would expect it to have asked her why she was making the payments, whether there was a third party involved and if so how she met them, whether she'd downloaded remote access software, whether she'd been promised unrealistic returns, whether she'd made any withdrawals, whether she'd been coached to lie, whether she'd done any due diligence and whether she'd been advised to make an onwards payment from the cryptocurrency exchange. And had it done so, I haven't seen any evidence that she'd been coached to lie and its clear she thought the investment was genuine, so I think she'd have explained she was investing in cryptocurrency with the assistance of a broker that she'd found on social media. With probing questions, I think she'd also have disclosed that the advert had featured a celebrity endorsement and that she'd been advised by the broker to download AnyDesk, which would have indicated to Revolut that she was being scammed.

I would expect Revolut to have provided a further warning tailored to cryptocurrency investment scams and advice on additional due diligence, but if Ms M had decided to proceed, as I'm satisfied Revolut would have had enough information to detect the scam, I would expect it to have gone a step further and told her how to check she was dealing with a genuine company, including contacting the details on the CySEC or FCA websites. And as I haven't seen anything to suggest she ignored any warnings or that she wouldn't have followed this advice, I'm satisfied she'd have discovered that J was operating was a scam.

Consequently, I'm minded to direct Revolut to refund the money Ms M lost from the fourth payment onwards.

Contributory negligence

I accept there's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence but, in the circumstances, I don't think Ms M was to blame for the fact she didn't foresee the risk.

This was a sophisticated scam and Ms M hadn't invested in cryptocurrency before and wouldn't have known that celebrity endorsements and the use of AnyDesk are red flags for fraud without a warning from Revolut. She had been given some very convincing documentation and had been reassured by the fact she'd received a small withdrawal and was able to see what she thought were her profits on J's trading account. Further, J was a clone of a genuine company and so any research she might have done would have further convinced her that the opportunity was genuine. So, I'm not minded to concluded that she should share responsibility for her own loss.

Recovery

Ms M'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 exchange would have been able to evidence they'd done what was asked of them. That is, in exchange for Ms M'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 Revolut's decision not to raise a chargeback request against the cryptocurrency exchange was fair.

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

Compensation

The main cause for the upset was the scammer who persuaded Ms M to part with his funds. I haven't found any errors or delays to Revolut's investigation, so I don't think she is entitled to any compensation.

Developments

Neither party has submitted any further evidence or comments or submitted for me to consider.

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.

Because neither party has submitted any further evidence or comments for me to consider, the findings in my final decision will be the same as the findings in my provisional decision.

My final decision

My final decision is that Revolut Ltd should:

• refund the money Ms M lost from the fourth payment onwards
• pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.
*If Revolut Ltd deducts tax in relation to the interest element of this award it should provide Ms M with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms M to accept or reject my decision before 8 April 2025.

Carolyn Bonnell
Ombudsman