DRN-5118776

The complaint

Ms H 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 July 2022, Ms H came across an advert on social media for an investment opportunity, which was endorsed by a well-known celebrity. She had never invested before and believed the advert was genuine.

After registering her interest, Ms H was contacted by someone I'll refer to as "the scammer" who said he worked for a platform I'll refer to as "P". He explained she'd be investing in cryptocurrency, and that she could start with a deposit of £219. Ms H did some basic research and was satisfied P seemed genuine and that there were no negative reviews.

The scammer asked Ms H to download remote access software so he could guide her through the investment process. He instructed her to open an account on P's platform, which required her to provide ID documents. He also instructed her to open an account with Revolut and to first purchase cryptocurrency through a cryptocurrency exchange company before loading it onto an online wallet.

Several credits were received into the Revolut account, which Ms H believed were funded by P. When she asked the scammer about the funds, he said the loans would be repaid and she'd have no liability for them. In fact, the scammer had taken out five loans in Ms H's name using remote access software. Ms H transferred funds to the Revolut account from Bank S and Bank C and between 21 March 2023 and 29 April 2023, the scammer processed nine faster payments and seven card payments to five different beneficiaries from the Revolut account using remote access software.

In March 2023, the scammer told Ms H that her initial investment had grown to £7,980 and so she asked to make a withdrawal. The scammer said she'd have to pay various fees and taxes to release money from her trading account. Between 23 March 2023 and 29 April 2023, she made payments which she understood were for commission, tax, and liquidity fees.

She realised she'd been scammed in April 2023, when she discovered that various loans had been obtained in her name and that this was this money the scammer had been sending to her Revolut account. She complained to Revolut, but it refused to refund any of the money she'd lost. It stated that it tried to recover the funds from the beneficiary account, but no funds remained, and that it wasn't liable for the transactions because it provided sufficient scam warnings.

Ms H wasn't satisfied and so she complained to this service with the assistance of a representative. She said she wasn't given any alerts or warnings until after 20 April 2023, and Revolut didn't question her about the payments or to provide advice about the risk of fraud. She said she isn't computer literate, so blog warnings are ineffective and Revolut failed to direct her initial complaint to the fraud department or advise her on the correct course of action over chargeback.

Her representative said Revolut should have intervened because there was a sudden increase in spending from a newly opened account, and multiple payments on the same day to new payees linked to cryptocurrency following credits from Ms H's external accounts. They said that if Revolut had contacted Ms H when she made the first payment on 21 March 2023 for £14,500 and advised her about investment scams, her loss could have been prevented.

They said Revolut should have asked probing questions to understand the context of the payments and why she'd taken out so many loans. They said she hadn't been prompted to give false answers and would have disclosed that she was acting under the instruction of a cryptocurrency trader, so it would have known the investment had the hallmarks of a scam and provided an effective warning. They further explained that the scammer told Ms H that if she was challenged about the payments, she should say she was sending funds to her sister who lived overseas.

Responding to the complaint, Revolut said its controls were proportionate and appropriate, Ms H must have authorised the transfers, and the card payments were authenticated via 3DS. It said that even though the account was created on 11 July 2022, it wasn't used at all until 10 months later, so there was no historical transaction behaviour that it could have considered to determine normal activity, and the stated account opening purpose was 'crypto', so transferring funds to crypto-related beneficiaries was normal and expected.

It said Ms H was shown a new payee warning each time she set up a new beneficiary stating and she was also shown a set of dynamic educational story messages to warn her about the risks associated with the payments. Ms H chose 'investment' as the account purpose and was given a tailored warning, in response to which she chose to proceed with the payment. Revolut further commented that communication with the scammer occurred via WhatsApp, which isn't commonly used by legitimate investment companies. It argued that she had ample opportunity to exercise caution because the scam occurred over a period of 52 days, and that the celebrity who'd endorsed the investment had a well-known association with scams, which was easily discoverable via some simple research, along with negative reviews about S.

Revolut said the fraudulent activity didn't take place on the Revolut platform and that the transactions were 'self to self' transactions, so for this service to effectively apply the reimbursement is an error of law. Alternatively, we have irrationally failed to consider the fact they are self-to-self and therefore obviously distinguishable from transactions subject to the regulatory regime concerning APP fraud. It has further argued that it is irrational (and illogical) to hold it liable for losses in circumstances where it is merely an intermediate link, and there are typically other authorised banks and other financial institutions in the payment chain that have comparatively greater data on Ms H. It said its likely Ms H was given warnings by Bank S because the funds were sent to Revolut, noting Ms H had said the scam started in June 2022, but the first payment from Revolut was on 23 March 2023, so she must have used other bank accounts to fund the investment.

Our investigator didn't think the complaint should be upheld. She noted the scammer had told Ms H the loans would be repaid and that she would have no liability for them and that she told Bank S that she'd taken out a loan to help her sister, so she did know about them.

She also commented that it wouldn't have been possible for the scammer to authorise the transactions using AnyDesk without some involvement from Ms H due to the various controls implemented within the Revolut platform. And the card payments were authorised via 3DS, so they couldn't have been completed without her permission. So, she was satisfied the transactions were authorised.

She noted the initial payment of £14,500 on 21 March 2023 triggered a warning and Ms H was asked to check the beneficiary details, warned about the risks associated with the payment, and asked to provide a payment purpose, which she confirmed as 'investment'. She was then warned '*Investment scams. Fraudsters could contact you, or you may see an advertisement online, offering you a fake but convincing – investment opportunity to make easy money. Are you being scammed? Legitimate investments will never guarantee a profit and won't be arranged over social media. Investment companies will be registered with a regulator, such as the Financial Conduct Authority (FCA) in the UK'.*

Our investigator didn't think this was sufficient because of value of the payment Ms H was making to a known cryptocurrency provider, and she thought it should have done more to establish the circumstances surrounding the payments. But she didn't think this would have made any difference because Miss H mislead Bank S when it intervened on 20 March 2023, which prevented it from detecting the scam.

She explained that the call handler had told Ms H that it was important she was honest, that criminals can be convincing, and that if she was asked by anyone to lie to the bank about the purpose of the payment then it will be a scam. She was asked if anyone had asked her to lie to or mis-lead her bank, and she said, 'no' before explaining that her sister lived overseas and was in trouble and she'd taken a loan out to help her. When questioned further she said '*they are helping with an animal sanctuary with veterinary care, and they've used all their money up. They need to pay bills and get the car back on the road, things like that. So, I said I would go out – as I'm not just going to transfer money without knowing exactly what they're doing. I'm going to book a flight and go out there to help'.* After a lengthy conversation, the payment was processed.

Similarly, Ms H told Bank C that the payments she was making from that account were to 'pay someone I know'. And there was evidence that she was being coached in the messages she had with the scammer, for example *'they might make it complicated as they see its credit funds. And you've been transferring lot lately. But remember this last transaction so push them to approve'.*

Our investigator noted that the story about her sister wouldn't have been plausible in response to questions from Revolut because Ms H was paying a cryptocurrency merchant, but she thought it was likely that she'd have been given a different cover story, so it wouldn't have been able to detect the scam. And she didn't think she'd have paid attention to any warnings.

Finally, she noted that although Revolut failed to raise chargeback requests for the card payments, as she'd used her debit card to buy cryptocurrency, it's unlikely a chargeback would have succeeded. She also explained that the transfers were sent to third parties to purchase cryptocurrency, which she had received, so there was no prospect of a successful recovery. And she didn't think Ms H was entitled to any compensation.

Ms H has asked for her complaint to be reviewed by an Ombudsman. Her representative maintains she didn't know about the loans at the point of application. They accept Ms H was coached to lie, but they have argued that she wouldn't have been able to lie to Revolut because she was paying a cryptocurrency merchant. They argue that Revolut should have

identified the account activity as suspicious and provided better warnings, and had it done so the warnings would have resonated with Ms H and her loss would have been prevented.

They also maintain Ms H didn't authorise or execute the transactions and have challenged Revolut's suggestion that the scammer couldn't have used AnyDesk to make the transfers without Ms H's involvement and they have argued that Revolut ought to have detected the use of remote access software.

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 Ms 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 understand that Ms H has said the payments were executed by the scammer using AnyDesk, but I'm satisfied she downloaded AnyDesk and gave the scammer permission to use it to access her device so he could guide her through the investment process. Significantly, there's evidence she was involved in the payments from Bank S to Revolut, and she has explained that she believed she was investing in cryptocurrency and would be purchasing cryptocurrency before sending it to an online wallet. Further, Revolut has stated that it's not possible to perform actions on an account when a screensharing application is being used. And the fact the card payments were authorised via 3DS means Ms H would have had to engage with the process either by sharing her security details or by using biometrics.

So, I'm satisfied, on balance, that she knew about the payments and that the transactions were authorised 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 H is presumed liable for the loss in the first instance.

Prevention

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

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 March 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 genuine cryptocurrency merchants. 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 did enough when Ms H 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 H from financial harm due to fraud.

The payments did flag as suspicious on Revolut's systems and so I've considered whether it intervened at the right time and whether the interventions were proportionate to the risk presented by the payments.

Ms H transferred £14,500 to S on 21 March 2023, and I agree with our investigator that some sort of intervention was appropriate because she was sending a significant amount to a merchant which was identifiably linked to cryptocurrency from an account that hadn't been used since its creation, having received funds into the account the day before. I've considered whether the warning Revolut gave to Ms H was proportionate to the risk and I agree with our investigator that it should have done more.

I think a proportionate response would have been for one of Revolut's agents to have contacted Ms H via its live chat facility and to have asked probing questions about the circumstances of the payments including whether there was a third party involved and if so how she'd 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.

However, as Ms H wasn't honest with Bank S when she was questioned about a payment she was making from that account on 20 March 2023, I don't think she'd have answered these questions honestly. I accept the story about her sister wouldn't have been plausible because she was sending funds to a cryptocurrency merchant, but I've no doubt the scammer would have coached Ms H not to tell Revolut how she came across the investment or that there was a third party involved, and without this information, it wouldn't have detected the scam.

In any event, because Ms H was sending such a large amount to a cryptocurrency merchant, I would still expect Revolut to have provided a written warning which was tailored to cryptocurrency investment scams and I note there were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Ms H's payments, such as finding the investment through an advertisement endorsed by a public figure, being assisted

by a broker and being asked to download remote access software. But Ms H had been convinced by the celebrity endorsement and its clear she was being guided by the scammer and trusted him to the extent that she followed his advice to mislead Bank S and Bank C.

And she went ahead with the first payment from Revolut having been shown a relevant warning and without having done any effective due diligence. So, I think that even if a more detailed warning had resonated with her, she'd have discussed it with the scammer, and he'd have reassured her the investment was genuine and that it didn't apply to her.

Significantly, I understand it was Ms H's difficulty in withdrawing money that led her to realise that she was being scammed and so I think that if Revolut provided Ms H with an impactful warning before she began to have those doubts, I don't think it would have made a difference.

I've considered whether there were any further opportunities to stop the scam, and I think Revolut should have intervened again when Ms H paid £24,000 to S two days later but there's nothing to persuade me the outcome would have been any different. And none of the later payments exceeded £24,000, so while the beneficiaries did change, sending funds to cryptocurrency merchants was no longer unusual, so there would have been no reason to intervene.

So, while I accept that Revolut could have done more on 21 March 2023 and 23 March 2023, I don't think these were missed opportunities to have stopped the scam.

Recovery

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

I've thought about whether Revolut could have done more to recover Ms H's 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. Revolut) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Ms H).

Ms H's own testimony supports that she used cryptocurrency exchanges to facilitate the payments. 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 Ms 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 Revolut's decision not to raise a chargeback request was fair.

Compensation

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

I'm sorry to hear Ms H 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 Ms H to accept or reject my decision before 17 June 2025.

Carolyn Bonnell
Ombudsman