DRN-5198216

The complaint

Mrs B complains that Revolut Limited ('Revolut') won't refund the money she lost when she fell victim to a scam.

What happened

Mrs B says that a friend of hers introduced her to a job opportunity with a company I'll call J. The job involved completing review tasks to increase the popularity of various products.

Mrs B was advised she needed to deposit funds on a platform to simulate buying items. To do this, she was asked to create a Revolut account and use funds from that account to buy cryptocurrency from a platform. That cryptocurrency was then moved to J's platform. On completion of sets of tasks, Mrs B was told she would receive commission and her deposited funds would be returned to her.

Between 26 December 2023 and 3 January 2024 Mrs B made fifteen card payments totalling £9,068 from her Revolut account to a cryptocurrency platform. The tasks became more expensive until Mrs B was unable to make further payments. She was told that she could not withdraw her funds without paying to complete the set of tasks. Mrs B realised she was the victim of a scam and contacted Revolut on 16 January 2024.

Revolut said that it had no valid chargeback rights in respect of the card payments.

Mrs B was unhappy with Revolut's response and brought a complaint to this service.

Our investigation so far

The investigator who considered this complaint didn't recommend that it be upheld. He noted that Revolut intervened when Mrs B made one payment and asked her some questions. After Mrs B confirmed that she was being guided on how to respond to Revolut's questions, she was directed to its chat. Whilst Mrs B then said she wasn't being guided, she did explain that she was making payments linked to a job and would receive commission. Given what Mrs B said, the investigator thought that Revolut should have done more than it did.

But, based on the messages Mrs B exchanged with the scammer and the conversations she had with the bank when she transferred funds to her Revolut account, the investigator concluded that further intervention wouldn't have stopped Mrs B from making the payments. Even after Revolut prevented Mrs B from making further payments, she found another way to proceed.

Mrs B didn't agree with the investigator's findings and asked for a final decision. Her representative requested recordings of the calls Mrs B had with her bank. Many of the points then raised by Mrs B's representative relate to perceived failings of Mrs B's bank, which aren't relevant here. But Mrs B's representative stressed that her bank didn't bring to life job scams or provide relevant or appropriate job scam warnings. So, if Revolut had set out the common features of a job scam, and discussed the fact the returns she had received were insignificant compared to the amount sent, and a common scam tactic, she would not have proceeded.

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.

When considering what is fair and reasonable, I'm also required to take into account: relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant time.

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 (2017) and the terms and conditions of the customer's account.

But, taking into account relevant law, regulatory 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 December 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;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- 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'm mindful that Mrs B's account with Revolut had only been opened recently so Revolut didn't have an understanding of Mrs B's normal account activity. There's also a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments. Whilst banks have obligations to be alert to fraud and scams and to act in their customers' best interests, they can't reasonably be involved in every transaction.

That said, Revolut did in fact intervene in the early days of the scam. On 28 December 2023 Revolut declined two payments of £251 which were made before a successful payment of the same amount. Mrs B was advised her payment could be a scam and was asked, "*Is anyone prompting or guiding you?*". Mrs B clicked the 'yes' box and was provided with educational screens which said:

You could be talking to a scammer

Sounds too good to be true? It probably is. End the call and stop all communications.

Beware of unusual requests

Scammers might ask your card details for many reasons. Never share your details!

Look for a second opinion

Scammers may impersonate banks, financial institutions, or others and ask you to approve transactions. Please be careful.

Revolut then forced Mrs B to communicate via its in-app chat. Before Revolut had asked any questions, Mrs B said it wasn't a scam. When asked for some additional details, Mrs B said, "*It's a job am doing*". She went on to say it was a legitimate job and she got her funds back, and that she completed tasks and had to add funds to get a bonus. Mrs B added that she had got funds back so it couldn't be a scam. She also provided a link to J's website.

In response, the Revolut agent provided impersonation scam warnings and then asked Mrs B who was guiding her. Mrs B said she clicked this box by mistake and was doing it herself. When asked if she was buying cryptocurrency, Mrs B said that she wasn't – and that the payment had nothing to do with cryptocurrency. The agent went on to ask about screen sharing and whether she had researched the company she was '*buying/investing on*". Mrs B confirmed she had. She added that it was on the website of a known recruitment company, it was a part-time job, and her friend was doing it too. Mrs B was given the following advice:

"*Make sure any research you do is your own – fraudsters create convincing looking posts on social media, or share articles about investing. If someone says you need to send money as a tax or fee to access your funds, you are being scammed. Are you comfortable with proceeding with this transaction?*"

After acknowledging that Revolut would be unable to recover her funds if she was the victim of a scam, and she was not being assisted, Mrs B's payment was processed.

I'm not persuaded that Revolut's intervention went far enough. Mrs B clearly explained that the payment, which was identifiably to a provider of cryptocurrency, related to a job. Her responses clearly raised job scam red flags, (she referred to completing tasks, to adding funds to get a bonus and to the job being part-time), but none of them were picked up on. Instead, Mrs B was provided with warnings that weren't relevant to her circumstances.

Even though Mrs B didn't mention investing at all, the Revolut agent referred to investing and provided a warning that related to it. The agent also accepted Mrs B's explanation that the transaction had nothing to do with cryptocurrency, when this was patently not the case given the payee.

Revolut should also have been mindful that cryptocurrency scams have become increasingly varied over the past few years. Fraudsters have increasingly turned to cryptocurrency as their preferred way of receiving victim's money across a range of different scam types, including 'romance', impersonation, investment scams and job scams.

When presented with responses which clearly indicated Mrs B may be falling victim to a task-based job scam, Revolut ought to have taken steps to ensure this wasn't the case. I consider a proportionate response would have been to provide a warning that set out the essential features of a scam of this nature. For example, Revolut could have explained that these scams might involve being approached via a messaging app with a part-time job/remote opportunity, making payments to gain employment, being paid for 'clicks', 'likes' or promoting products, and having to pay increasingly large sums without being able to withdraw any money.

I've gone on to think about whether such a warning would have prevented Mrs B's loss from the point of intervention onwards. On balance, I'm not persuaded that it would and will explain why.

I've listened to three calls Mrs B had with her bank just after Revolut intervened on the £251 transaction. I'm not assessing the involvement of Mrs B's bank. Instead, I'm considering if the content of the three calls leads me to fairly conclude that it's more likely than not that a warning tailored to task-based job scams in Revolut's chat would have prevented Mrs B's loss.

During these calls, Mrs B's bank discussed with her payments to her Revolut account. Mrs B was open in saying that the payments related to a part-time job that a friend had introduced her to (and had shown her the research she completed), that she would receive a bonus and

profits for completing tasks, and that she had been able to withdraw funds. The advisers Mrs B spoke to raised serious concerns about what she was doing and how suspicious it sounded, and one went as far as saying they thought she was the victim of a scam (although not a job scam). They also spoke about the scammer's tactic of returning funds to persuade a victim to pay more in before not allowing withdrawals, which is what happened here.

Mrs B said she understood her bank's concerns but was clear that the role had been advertised on the site of a known recruitment company, her friend had been doing the job for some months and she had spoken to her friend about it, and she had been able to withdraw funds twice. She wanted the payment to be made and made it clear she would take responsibility for the loss if it turned out to be a scam. Given Mrs B's conviction in the face of clear suspicion and concern, I'm not persuaded warnings in Revolut's chat would have resonated with Mrs B.

It's also unclear if Mrs B would have been open in her responses to further questions. She told Revolut she'd incorrectly said that someone was helping her and later said the transactions were unrelated to cryptocurrency – which clearly wasn't the case.

After Revolut's intervention on 28 December 2023 Mrs B continued to make payments to the same cryptocurrency exchange. Initially they were relatively low in value (£312 and £438 on 28 December). On 31 December 2023 Mrs B made multiple payments to the same cryptocurrency provider (£558, £30, £1,130, £1,600, £30, and £1,790). Given what Revolut knew about the reason for the payments, and the pattern of them, I consider Revolut ought reasonably to have had concerns and taken additional steps before processing the £1,600 transaction. I think a proportionate response to the risk posed would have been to ask a series of questions to narrow down the scam risk and to provide warnings tailored to the risk identified.

I've thought carefully about whether an additional intervention at this point would have prevented Mrs B from making further payments. Whilst I accept that Mrs B's bank hadn't told her she was likely falling victim to a job scam, it had expressed real concerns and had told her it thought she was being scammed. Mrs B didn't take any additional steps to check the legitimacy of the job offer but relied on her relationship with the friend who introduced her. I consider it more likely than not that she would have continued to do so and that she wouldn't have heeded additional warnings from Revolut.

Mrs B's representative has said she was vulnerable at the time the scam payments were made. I can't see that Mrs B made Revolut aware of this and am mindful that the account was newly opened. Overall, I'm not satisfied Revolut had any reason to believe Mrs B needed any additional support.

Finally, I've considered whether there was any way Revolut could have recovered Mrs B's funds. The transactions were made by card which offers some protection. But, as the merchant provided the cryptocurrency paid for, a chargeback wouldn't have been successful.

Overall, whilst I'm very sorry to hear about Mrs B's loss, I can't reasonably ask Revolut to reimburse her.

My final decision

For the reasons stated, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs B to accept or reject my decision before 30 April 2025.

Jay Hadfield
Ombudsman