DRN-4552151

The complaint

Miss H complains Revolut Ltd didn't do enough to protect her when she fell victim to a job scam.

What happened

Miss H fell victim to a task-based employment scam ('job scam') in June 2023. Miss H was looking for opportunities to work from home, to provide her with an additional income. She recalls clicking on a link on a job advertisement and immediately receiving a WhatsApp message from someone ('the scammer') purporting to be recruiting for a legitimate company ('C'). Miss H was then directed to another website (which was similar to the genuine company's address but was in fact a clone of the genuine C) which she was advised was the employee portal. Miss H said she carried out some research into C and satisfied herself the job opportunity was legitimate.

The scammer directed Miss H to open a work account with C, which required her to satisfy various know your customer (KYC) and anti-money laundering (AML) checks. Miss H was also directed to join a WhatsApp group with a group of other individuals who were supposedly doing the same job. Miss H was instructed to open an account with, and transfer money to, Revolut. She was also told to set up an account with a legitimate crypto exchange platform ('B') and purchase crypto, which she then transferred into her work account with C. Miss H was led to believe that she would receive back her funds plus any commission made.

Miss H was told she would be required to complete a set of 65 tasks each day, which involved rating products to boost their marketing. On completion of the tasks Miss H was told she would receive commission, which she could see on her work account, that would be paid in crypto. Miss H said she was initially able to successfully complete the tasks and on the first day she received a credit of £273.76 for the work she had completed. But the following day she received a 'premium task', which put her account into a negative balance. She was then required to deposit further funds into her working account to complete the remaining tasks.

Between 25 and 27 June 2023, Miss H made ten card payments to B totalling £5,558.54 (including fees), and received one credit from it:

Payment number	Date and time	Payment type	Amount
1	25 June 2023 at 11:14	Card payment	£100
	25 June 2023 at 13:27	*Credit from B*	*(£273.76)*
2	26 June 2023 at 11:04	Card payment	£200
3	26 June 2023 at 11:52	Card payment	£267.70
4	26 June 2023 at 11:59	Card payment	£60
5	26 June 2023 at 13:08	Card payment	£606.68
6	26 June 2023 at 13:34	Card payment	£1,260.62 + £11.35 fee
7	26 June 2023 at 13:14	Card payment	£47.26 + £0.47 fee
8	26 June 2023 at 15:21	Card payment	£275.47 + £2.75 fee

9	27 June 2023 at 11:33	Card payment	£3,000
		Total loss	£5,558.54

Prior to making the final £3,000 payment, Miss H had attempted a number of other card payments and transfers from her account with Revolut but they were declined or failed. Revolut has explained that at this time it had partially restricted Miss H's account as it needed to verify the source of one of the payments that credited her account. It emailed Miss H on 26 June 2023, and it removed the restriction when she provided the required information on 27 June 2023.

Miss H said she realised she'd been scammed when she received further premium tasks, which she thought were unreasonable and she could not fund as she had run out of money. She was then pressurised by the scammer to make further payments and told her account would be frozen until she made the further payments. She reported the matter to Revolut and asked for help recovering the funds. Revolut advised her to raise a chargeback claim, although these were ultimately unsuccessful as Miss H had authorised the payments from her account using 3DS.

Unhappy with Revolut's response, Miss H referred her complaint to the Financial Ombudsman with the help of a professional representative. Our Investigator didn't uphold the complaint. While she considered Revolut ought to have presented Miss H with a warning that highlighted the risks of crypto investment scams, she did not think this would likely have resonated with Miss H as this was not the scam she was falling victim to. She thought it was most likely that even if presented with a crypto investment warning Miss H would have continued to make the payments.

Miss H's professional representative disagreed and asked for an Ombudsman's final decision. It considered that Revolut ought to have spoken with Miss H when it had concerns about the declined and failed payments to understand what the incoming payment was for, as well as to verify the payments from her account. It said it should also have been concerned that Miss H had made seven payments to B in the space of 24 hours.

Our Investigator disagreed. She noted that the evidence supported that Revolut's only concerns at the time were the source of funds. She did not think there was reason to expect Revolut to have spoken with Miss H about the £3,000 payment before processing it, although she would have expected it to present a warning.

As there has been no agreement the case has been passed to me to decide.

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 learn Miss H has been the victim of a sophisticated scam, which caused her to lose money. I don't underestimate the impact this has had on her, and I can understand why she wants to do all she can to recover the money she has lost. But I can only direct Revolut to refund her losses if it can fairly and reasonably be held responsible for them.

Should Revolut be held liable for Miss H's loss?

In line with the Payment Services Regulations 2017 (PSRs), the starting position is that Miss H is liable for payments she authorises – and Revolut generally would be liable for unauthorised payments taken from her account.

There has been no dispute that Miss H made the payments herself. So, although she didn't intend the money to go to the scammers, under the PSRs Miss H is presumed liable for her loss in the first instance.

In broad terms, the starting position in 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 PSRs 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 June 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 – (as in practice Revolut sometimes does including in relation to card payments);
- 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.

But, with that in mind, there is also a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments.

So, the starting point for me is to consider whether any of Miss H's payment instructions – taken either individually or collectively - were particularly unusual or suspicious to have required intervention from Revolut.

I understand that Miss H opened the account with Revolut on 25 June 2023, on the instruction of the scammer to enable her to pay into her work account with C. As such, Revolut did not know her typical spending patterns. But that doesn't mean it wasn't able to recognise suspicious activity – only that the information it had on which to make that assessment was limited.

I've thought about what Revolut did know about Miss H when she came to make the first payment. That information was limited. Other than the payment amount and destination, it knew her personal details and that the account had been set up that day. When opening the account Miss H had stated her account opening purpose was *"Rewards"*.

The value of the initial payment (£100) was not at a level that I would have expected Revolut to have considered unusual or high risk. And while the payment went to a crypto exchange, again I don't think this ought to have given Revolut particular cause for concern. I'm mindful that customers of Revolut can purchase and trade crypto through its application. So, I don't

think it would appear unusual for a customer to use their account to purchase crypto. I don't therefore think Revolut ought to have intervened in Miss H's initial payment.

Similarly, the next seven payments were again not of values that I consider Revolut ought to have considered unusual or high risk. While I'm mindful that there were multiple payments in one day, I don't think it was necessarily apparent from this that Miss H was at risk of financial harm from fraud. I don't consider the sequence of payments were particularly suggestive of a scam at that stage, given the payments fluctuated in value and times.

But even if I considered Revolut ought to have been alerted to these payments at the time, I think a proportionate response would have been to present a written warning highlighting the key risks of crypto investment scams. But, for the reasons I'll go on to explain, I don't consider this proportionate intervention would have prevented the scam.

Like our Investigator, I'm satisfied that Revolut ought to have recognised that Miss H's final card payment (£3,000) carried a heightened risk of financial harm from fraud. I say this because it was considerably larger than the previous payments and exceeded the total value of the payments made on the previous days.

While I think Revolut ought to have recognised that Miss H was at heightened risk of financial harm from fraud when making this payment, I don't think any proportionate intervention by Revolut would have prevented Miss H's loss. I'll explain why.

I understand Miss H's representatives consider that Revolut ought to have gone further than just presenting Miss H with a warning at this stage. They have suggested that Revolut ought to have prompted a human intervention with Miss H where she was required to answer questions with an agent from Revolut. But I don't think this was proportionate to the risk identified at the time. While Revolut had some concerns about the source of funds crediting the account, it was able to satisfy itself that the source was legitimate following receipt of the information provided by Miss H. I don't consider this interaction ought to have made Revolut more concerned about the subsequent payment from her account, given the information from Miss H highlighted no further cause for concern.

As such, given what Revolut knew about the payment, it's value and that it was going to a crypto provider, I think a proportionate response would have been to present Miss H with a tailored written warning that highlighted the key risks associated with crypto payments at the time.

At the time of Miss H's payment the key scam risk concerned crypto investment scams. These operated in a different way to job scams and so I would not expect the warning to have resonated with Miss H. For example, a crypto investment scam warning may have highlighted that scammers will often make unsolicited contact, often through social media. This did not apply to Miss H as she believed she had been contacted by a legitimate recruitment agent while she was actively looking for work. Similarly, the risks about investing in crypto would not have resonated given that's not what she believed she was doing.

As such, even if Revolut had intervened as I'd have expected it to do, I'm not persuaded this would have prevented the scam and I think it most likely that Miss H would have continued with the payments. As such, in the circumstances, I don't think Miss H's losses could have been prevented.

I have a great deal of sympathy for Miss H and the loss she's suffered. But it would only be fair for me to direct Revolut to refund her loss if I thought it was responsible – and I'm not persuaded that this was the case. So, while I know this will be very disappointing for Miss H, I don't find that Revolut are responsible for her loss. It follows that I will not be asking it to take any further action.

My final decision

For the reasons given above, my final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss H to accept or reject my decision before 5 August 2024.

Lisa De Noronha
Ombudsman