DRN-4101965

The complaint

Miss S complains about Revolut Ltd.

She says that Revolut didn't do enough to protect her when she became the victim of a scam and would like Revolut to pay her back the money she has lost.

What happened

Miss S came across an advert for making investment in cryptocurrency on Facebook.

She made contact with the 'company' and was persuaded to purchase crypto. In total, she made three payments to 'W' (a seller of crypto) of €4,432.05, £4,327.69, and £1,145.27.

Once Miss S realised she had been the victim of a scam, she complained to Revolut, but it didn't uphold her complaint. Miss S then brought her complaint to this Service.

Our Investigator consider the complaint but didn't think that it should be upheld. I have previously issued a provisional decision on this complaint where I explained that I intended to partially uphold Miss S's complaint.

Miss S accepted my provisional decision, but Revolut did not.

Revolut has provided further commentary on receipt of my provisional decision, which I will comment on, but it hasn't persuaded me to change my opinion on the complaint.
So, I will now issue my final decision, which contains my provisional decision with extra commentary on the points Revolut raised.

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.

Was Miss S the victim of a scam?

I don't think it is in doubt here that Miss S was the victim of a scam – she responded to an advert she saw online and was persuaded to invest in crypto – however when she came to realising her supposed profit the scammer asked for more money in order to access this. This is not the action of a genuine investment provider.

Did Miss S authorise the payments?

In line with the Payment Services Regulations 2017 (PSRs), Miss S isn't liable for payments she didn't authorise, unless she failed with gross negligence or intent to comply with the terms of the account or keep her personalised security details safe.

Miss S made the payments to purchase crypto from W with her debit card herself, so I think that it's clear that she authorised them. I understand Miss S had been tricked into instructing

Revolut to make the payments – but while Miss S never intended the payments to go to the scammers, this doesn't change the fact she authorised them and is therefore presumed liable for the loss in the first instance.

Recovery of Miss S's payments

After Miss S made her payments, I wouldn't expect Revolut to do anything further until it was notified of the scam.

All of Miss S's payments were made by debit card - so the only recourse for potential recovery would be by via the chargeback scheme. Chargeback is a process by which disputes are resolved between card issuers (here, Revolut) and the merchant (here, W). But it's very unlikely that a chargeback would ever have seen successful.

This is because W is a legitimate company and provided the services that Miss S requested – the purchase of crypto and subsequently moving that crypto onto a wallet of Miss S's choosing. What happened after that crypto was successfully moved is therefore a separate matter – so a successful chargeback would likely not have not possible – and I don't think that these payments were recoverable once they had been made.

Should Revolut have reasonably prevented the payments in the first place?

I can only uphold this complaint if I think that Revolut reasonably ought to have prevented some or all of the payments Miss S made in the first place – therefore preventing the loss before it happened.

Miss S authorised the scam payments in question here – so as I've explained above, she is presumed liable for the loss in the first instance.

That said, as a matter of good industry practice, Revolut should have taken proactive steps to identify and help prevent transactions – particularly unusual or uncharacteristic transactions – that could involve fraud or be the result of a scam. However, there is a balance to be struck: banks had (and have) obligations to be alert to fraud and scams and to act in their customers' best interests, but they can't reasonably be involved in every transaction.

Taking into account the law, regulatory rules and guidance, relevant codes of practice and what I consider having been good industry practice at the time, I consider Revolut should fairly and reasonably:

- Been monitoring accounts – including payments made and received – to counter various risks including anti-money laundering, countering the financing of terrorism and preventing fraud and scams;
- Have had systems in place to look out for unusual transactions or other signs that might indicate its customers were at risk of fraud (amongst other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer; and
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

So, I've carefully considered what this means for Miss S and the payments in question here The first payment Miss S made to W for €4,432.05. Miss S thinks that Revolut should have intervened from this payment. I've carefully considered this, but I'm not persuaded to agree

here.

I can see by looking at Miss S's statement that her account with Revolut was not used that regularly – and appears to have been used for converting and sending payments in Euro, rather than day to day transactions, which may have allowed Revolut to build up a picture of Miss S's regular account activity in order to identify suspicious patterns. While the payment was much higher than 'normal' for this account – I can't say that it was so unusual that Revolut should have intervened here - not every payment to a company selling crypto is a scam and as I've said above, there is a balance to be struck.

However, Miss S then made another payment, only a few days later for £4,327.69. This clearly indicates a marked change in the way that Miss S was operating her account. I think that this payment should've triggered a response from Revolut in order to meet its obligations I've set out above. With this in mind, Revolut should reasonably have contacted Miss S to establish whether the transaction posed any possibility of placing Miss S in financial harm before processing it. But it did not do so.

Had Revolut contacted Miss S, I would've expected it to have questioned Miss S about the payment – including what the payment was for, and the surrounding context – and to proceed accordingly. The intention being to disrupt or uncover a potential fraud or scam.

I've seen nothing to suggest that Miss S had been coached, or told to lie about the payments she was making – so I think that had Revolut acted as I would've expected, it would quickly have uncovered that Miss S had made contact through Facebook with a company offering investment in crypto – and had been persuaded to download AnyDesk onto her computer. I think she would also have told them that the scammer used AnyDesk to move the crypto she had purchased onto another wallet.

Revolut has said that the payment reference used by Miss S when transferring the money from her bank 'H' to Revolut was *'holiday'* which shows that Miss S took steps to conceal the true nature of the payments, and had likely been coached to provide an answer to Revolut had it intervened. But it is my understanding that when a new payee is set up, a payment reference is chosen for the first transaction, and continues to be the same unless a customer chooses to amend this. And as Miss S was using her Revolut account for converting and making payments in Euro, it is not unreasonable to think that this is the reference she chose when first making her payments and simply never opted to change this once the link had been set up.

By January 2019, Revolut should already have had a good understanding about how scams like the one Miss S fell victim to work – including that a consumer is often persuaded to move money from one crypto-wallet in their own name to the scammer. Had Revolut given Miss S a meaningful warning that what she had told it bore all the hallmarks of a sophisticated scam – I think that she would've taken this warning seriously and not taken the risk of continuing with the payment.

I understand that Revolut says that Miss S's account was not a current account – and that it is not a bank but an Electronic Money Institute (EMI). It says that this type of account is opened and used to facilitate crypto payments – and that the payments to W are not out of character with the typical way in which an EMI account is used. It also says that once a payment had been made to W that it became an established merchant, which made further transactions less unusual, and that the payments were spaced out.

But an EMI account isn't only used for the purchase of crypto – and Miss S had been using the account for converting and sending payments in Euro – so the payments to purchase crypto were unusual for Miss S (although as I've said above, I don't think that there was

enough for Revolut to intervene from the first payment) – and the second payment was only a few days later.

Revolut also says that the payments were made to a crypto account in Miss S's own name, and so the scam Miss S fell victim to is out of the scope of Revolut and should be directed to the seller of the crypto. But as I've explained above, Revolut missed an opportunity to uncover the scam here, and as it is aware, the seller of the crypto does not have the same obligations as it has – and is not regulated in the same way.

Finally, Revolut also says that Miss S's bank 'H' (which was used to fund Miss S's Revolut account) should be partially liable here as it would have had a better understanding of her spending and the transactions would have been more suspicious when being transferred to Revolut. But I disagree.

This Service isn't considering a complaint about H – but this isn't required for me to consider the complaint in hand here. Revolut was an established payee of Miss S – and she had funded her Revolut account via H for a long time prior to when the scam began. So only Revolut could have known about the change in Miss S's spend from her account with it – and H wasn't aware of any activity taking place on her account with Revolut.

So, nothing Revolut has said here changes my opinion, and I still think that Revolut could have stopped the payments from payment two had it intervened as it ought to have done.

Putting things right

Revolut Ltd should pay Miss S £5,472.96

It should also pay Miss S 8% simple interest, per year, on this amount the date of payment to settlement (less any tax lawfully deductible).

My final decision

I uphold this complaint in part. Revolut Ltd should put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss S to accept or reject my decision before 25 May 2023.

Claire Pugh
Ombudsman