DRN-4004098

The complaint

Mrs S complains that Revolut Ltd won't refund money she lost when she was a victim of a scam.

Mrs S is represented by a firm that I'll refer to as 'C'.

What happened

The background to this complaint is well known to both parties and so I'll only refer to some key events here.

In late 2022 Mrs S contacted a well-known and popular investor on a social media platform that offered mentoring programmes. After receiving a response, Mrs S asked for a few days to consider whether she wanted to proceed with the one-to-one training. A couple of days later Mrs S received a follow request from what appeared at the time to be the same social media account. The person ('scammer') contacting her however was impersonating the genuine account – with an almost identical username.

The scammer convinced Mrs S to invest and assisted her in setting up an account with a legitimate crypto exchange as well as a profile with the investment platform. After seeing profits from the initial investment, the scammer was told she had to pay various fees to release the money. These payments were made via legitimate crypto exchanges. The relevant payments are:

Date	Type	Payee	Amount
24 November 2022	Debit card transaction	Crypto Exchange A	£200
25 November 2022	Debit card transaction	Crypto Exchange A	£800
25 November 2022	Debit card transaction	Crypto Exchange A	£2,500
26 November 2022	Debit card transaction	Crypto Exchange B	£4,300
26 November 2022	Debit card transaction	Crypto Exchange B	£550
26 November 2022	Debit card transaction	Crypto Exchange B	£2,000
27 November 2022	Debit card transaction	Crypto Exchange C	£350
		Total:	£10,700

Mrs S received credits into her account, of £66.09 and £72, on 24 and 30 November 2022 respectively.

C complained to Revolut, on behalf of Mrs S, on 5 December 2022 saying these payments were made as part of an investment scam. They considered Revolut failed in their duty of care to protect Mrs S from it by not identifying the above payments as unusual and suspicious, thereby warranting further investigation and enquiries. C said, had such enquiries been made, Revolut would've become aware that Mrs S was likely the unfortunate victim of a scam. And upon being appropriately warned of the risks involved, Mrs S wouldn't have proceeded with making the payments but instead, she would've sought to establish whether the investment opportunity was genuine. Because of this, C wanted Revolut to reimburse Mrs S her loss from the scam.

Revolut didn't uphold the complaint. They said they were actively trying to assist Mrs S and attempted to contact her via their in-app chat, as part of their investigation, but she didn't respond. And they would need further information from Mrs S to start their investigation and attempts to recover funds. Revolut requested Mrs S contact them to provide the necessary information and added that they're acting in accordance with regulatory requirements.

Our Investigator considered the complaint but she didn't think Revolut had to do anything further. In short, she said:

- She didn't think the payments were particularly unusual or suspicious to Revolut, thereby requiring them to intervene before processing them. This was because the account was newly opened and so there wasn't any account history to evidence Mrs S's typical spending – which makes it more difficult for firms to identify when a customer is at risk of financial harm from fraud.
- Making payments to new payees on a new account isn't reason enough for Revolut to have intervened, as a new account would likely involve payments to new payees.
- She also didn't think the transactions were so large that Revolut should've intervened without the benefit of Mrs S's typical spending history. And, while there were multiple payments for crypto purposes over a few days, by the time Mrs S made the larger payments – such as the £4,300 – her typical account usage involved making payments involving crypto. So, given the payments didn't flag as suspicious and Mrs S didn't speak with Revolut when making the payments, she didn't think Revolut missed an opportunity to prevent the loss suffered.
- Although some banks have decided not to let their customers make payments to the crypto exchange, this doesn't mean all consumers using it are at risk of being scammed. And it's Revolut's discretion as to whether to they allow this or not.
- Electronic Money Institutions (EMI) – like Revolut – weren't involved in the creation of the British Standards Institution (BSI) code (PAS 17271). And so, there are different obligations between EMIs and banks as to when they should intervene to protect customers from financial harm from fraud.
- It's not unusual for consumers to use EMIs differently to current accounts with banks. This includes, as happened here, money being paid into the account before being used for the crypto payments. So, she didn't think the payments were remarkable enough to stand out to Revolut given that nothing else about them differed from how other customers typically use EMIs.
- She thought it was reasonable for Revolut not to raise chargeback claims on the payments as she didn't think there were reasonable prospects of success. This was because the claims would've been against the crypto exchange and trading platforms for which she received a service – that being the purchase of crypto.

C disagreed and so the matter has been passed to me to decide. In short, they said:

- They consider the payments made from the newly opened Revolut account should've been recognised as suspicious according to the BSI code. The payments were of a high amount and going to a series of new payees linked to crypto, matching the prevalent pattern of investment fraud. Revolut therefore should've been alerted to them and to the fact Mrs S was being targeted to a sophisticated investment scam.

- Although they appreciate the usage patterns and trigger points are different for EMIs to banks, they maintain these transactions were sufficiently unusual to have indicated a high risk of financial harm.
- Mrs S repeatedly made large deposits into the Revolut account before rapidly using the funds to purchase crypto by making payments to new payees. Revolut ought to have least sought to have established the source of these substantial funds for anti-money laundering purposes. Over £10,000 passed through the account entirely unchallenged – which demonstrates Revolut failed to monitor the account for countering both risks involving money laundering and scams.
- Although they recognise Revolut's customers utilise their services to legitimately invest in crypto, they stressed that the fact these numerous payees were related to crypto is just one indicator of financial fraud. The payments were also unusual as they were made in short succession and of an increasingly high value -- which follows a known pattern of financial fraud in investment scams that Revolut ought to be aware of but missed here.
- They dispute the notion there needs to be historic spending on an account to compare activity to detect potentially fraudulent transactions. They think this activity strongly mirrors the hallmarks of typical investment scams and so, they consider Revolut should've intervened and broken the spell of the scammer – thereby preventing the financial and mental impact on Mrs S caused by it.

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.

I'm sorry Mrs S has been the victim of a scam and I don't underestimate the impact this has had on her. However, I must consider whether Revolut is responsible for the loss she has suffered. And while I know this won't be the outcome Mrs S is hoping for, I don't think they are. It follows that I don't think Revolut has acted unfairly by not refunding the money lost. I'll explain why.

In broad terms, the starting position in law is that an EMI is expected to process payments that their customer authorises them to make. It isn't disputed that Mrs S knowingly made the payments from her Revolut account and so, I'm satisfied she authorised them. Therefore, under the Payment Services Regulations 2017 and the terms of her account, Revolut are expected to process the payments and Mrs S is presumed liable for the loss in the first instance.

However, taking into account the law, regulatory rules and guidance, relevant codes of practice and good industry practice, there are circumstances where it might be appropriate for Revolut to take additional steps or make additional checks before processing a payment to help protect customers from the possibility of financial harm from fraud.

So, the starting point here is whether the instructions given by Mrs S to Revolut (either individually or collectively) were unusual enough to have expected additional checks being carried out before the payments were processed.

Mrs S opened the Revolut account on 23 November 2022, the day before she started making payments to the scammer. Because of this, there wasn't historical spending on the account to have allowed Revolut to assess whether the scam payment transactions were

unusual for Mrs S. I've therefore thought about whether the payments themselves, without any typical account usage available, were suspicious enough to have prompted Revolut to consider Mrs S was at risk of financial harm from fraud.

C has referred to the payments being of a high value, going to new payees for crypto purposes and that they match a prevalent pattern of investment fraud. I think it would be relevant to note at this point that the scam payments were made by debit card – so not by fund transfer that would've involved setting up a new payee. And given it was a newly opened account, any transactions on the account would've been made to a new beneficiary. So, I don't think it can be reasonably said the payments ought to have stood out in this respect.

Although EMI accounts can be used in a similar way to a high street bank account, they often offer different services. And the services Revolut offer includes money transfers for crypto investment purposes – which many banks limit or restrict. So, while I accept scams like what Mrs S fell victim have sadly becoming increasingly prevalent, many of Revolut's customers will use their services to legitimately invest in crypto. I therefore don't think the payments being linked to crypto alone would've given Revolut sufficient reason to think Mrs S was at

I have however given careful consideration to both the value and pattern of the payments. Revolut do have a duty of care to protect their customers from financial harm from fraud. And looking at the payments here, I can see they were made over a period of four days with the first four payments also increasing in value (from £200 up to £4,300). But while a series of payments increasing in value over a short period of time can be an indicator of potential fraud, I'm not persuaded – in these specific circumstances – the payments were of a high enough value or sufficiently suspicious to have indicated a heightened risk of financial harm.

This is because, as I've said, there wasn't any typical account usage available for Revolut to assess whether the scam payment transactions were unusual for Mrs S. And I don't think Mrs S using funds to purchase crypto that she'd only recently deposited into her Revolut account could be said to be either out of character or particularly unusual. Nor do I think the payments were of a significant enough value, either individually or collectively, to have given Revolut cause for concern. I therefore think it was reasonable for Revolut to assume the payments were being made for legitimate crypto purposes. And so, it follows that I wouldn't have expected Revolut to have taken additional steps or carry out additional checks before processing the payments.

On a further note, I'm aware that C has also referred to Revolut's failure to appropriately monitor Mrs S's account for anti-money laundering reasons. They consider Revolut should have at least sought to establish the source of the funds Mrs S was using and, had they done so, they would've been able to question the payment(s) and identify the scam. Given I've no reason to think Mrs S funded the crypto purchases using illegitimate money, I can't reasonably conclude Revolut failed in respect of their anti-money laundering obligations. And so, I can't say they missed an opportunity to prevent the loss Mrs S suffered.

I've considered whether, on being alerted to the scam, Revolut could reasonably have done anything to recover Mrs S's losses, but I don't think they could. The only possible option for recovery here, given the payments were made by debit card, would have been via chargeback claims. But given these payments were for the purchasing of crypto with legitimate firms, I don't think chargeback claims would have been successful as Mrs S received the service she paid for. As such, I think it was reasonable for Revolut not have raised chargeback claims here.

I have a great deal of sympathy for Mrs S and the loss she's suffered. But it would only be fair for me to direct Revolut to refund her loss if I thought Revolut was responsible – and I'm not persuaded that this was the case. For the above reasons, I think Revolut has acted fairly and so I'm not going to tell them to do anything further.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs S to accept or reject my decision before 2 August 2023.

Daniel O'Dell
Ombudsman