

The complaint

Miss N complains that Revolut Ltd won't refund money she lost to a scam.

What happened

Miss N fell victim to a cryptocurrency investment scam. She came across a firm, which I'll refer to as 'MT', via an advert on social media. As part of the scam, Miss N was persuaded to open a Revolut account, which she did on 27 April 2023. She made card payments to a legitimate crypto exchange before forwarding the crypto on as part of the scam to MT. The relevant payments are:

Date	Payment type	Amount
27 April 2023	Debit card payment	£1,497.13
2 May 2023	Debit card payment	£264
3 May 2023	Debit card payment	£336
4 May 2023	Debit card payment	£300
9 May 2023	Debit card payment	£1,500
11 May 2023	Debit card payment	£600
15 May 2023	Debit card payment	£2,700
23 May 2023	Debit card payment	£1,492.12
25 May 2023	Debit card payment	£1,192.67
	Total	£9,881.92

Miss N realised she'd been scammed when she was advised to pay further fees to withdraw her investment profits. When she attempted to make a withdrawal without paying the fees the scammer stopped responding to her.

Miss N initially reported the matter to Revolut, but before it responded she instructed a professional representative ('C'), who wrote to Revolut to complain. C said Revolut had failed in its duty to protect Miss N from the risk of financial harm from fraud.

Revolut responded to Miss N's complaint explaining that it could not raise a fraud chargeback as the payments had been correctly authorised and authenticated via 3DS. It would therefore not reimburse her for the loss.

Miss N referred the matter to the Financial Ombudsman. She argued Revolut ought to have considered the transactions which debited her account to be suspicious given the volume of transactions and that the payments were linked to a crypto provider. She said Revolut should therefore have intervened and provided her with effective warnings before processing her payments. She asked for a full refund of her losses, plus interest and compensation.

Our Investigator didn't uphold the complaint. He was satisfied that Miss N had authorised the payments. Given what Revolut knew about the payments, our Investigator didn't think it ought to have been unduly concerned about the risk of fraud, and so it wasn't necessary to carry any further checks before processing the payments. He was also satisfied that a chargeback would be unsuccessful as Miss N was provided with the crypto she purchased.

C disagreed on Miss N's behalf. It argued that the transactions should have appeared unusual and suspicious as the account was newly opened, Miss N made several payments to two different crypto exchanges over several days and a pattern was emerging where Miss N topped up the account before making large payments out of the account leaving a minimal balance on each occasion. C also suggested that Miss N's payment may have been at odds with her stated account opening purpose.

As there's been no agreement, the case has been passed to me for a final decision.

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.

The starting position under the relevant regulations, the Payment Services Regulations 2017 ("PSR 2017"), is that Miss N is responsible for payments she's authorised.

So, I'm left to consider whether, taking into account regulators' rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, Revolut should have identified any of the transactions as particularly suspicious, such that some form of intervention ought to have taken place before the transactions were allowed to debit Miss N's account.

Where a firm like Revolut does have grounds to be concerned about a payment, I think it should reasonably take steps to warn its customer about the risk of proceeding. Whether a warning should be provided (and, if it should, the nature and extent of that warning) should be proportionate to the risk the payment presents. A balance must also be struck between trying to protect customers and not unduly inconveniencing them. I must also take into account that applying significant friction to all payments would be very onerous and impractical for Revolut and would result in the warnings themselves having less impact as they would be seen as 'the norm'.

Revolut did not have a previous customer relationship with Miss N. It did not know her typical spending patterns. But that doesn't mean it wasn't in a position 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 N when she came to make the first payment. That information was fairly limited. It knew her personal details, that she stated the reason for opening the account was "Transfers", that her account was new and that she was paying a cryptocurrency provider.

Miss N's representatives argue that the activity Miss N carried out was, in and of itself, typical of fraud: the opening of a new account, the deposit of funds and a payment to a crypto provider. But I don't find it surprising that a customer would open a Revolut account and use it immediately for a specific purpose. And, given that customers of Revolut can purchase and trade crypto through its application, it's likely that many customers will open Revolut accounts in order to purchase crypto. So, I don't find that this pattern of activity is necessarily indicative of fraud. And when considering whether a payment should trigger an intervention, at the time this payment was made, I think it was fair for Revolut to take into account a range of factors, not just that the payments were going to a crypto provider. And while I can see Miss N did not specifically select "Cryptocurrency" as her account opening purpose, I also don't think her selected purpose – "Transfers" – was necessarily contradictory or should have given Revolut any further cause for concern.

Overall, I can't see that there was sufficiently concerning information about any of Miss N's payments that Revolut ought to have intervened or provided a specific warning before processing the payment instructions. So, while I know this will be disappointing for Miss N, I don't find that Revolut are responsible for her loss.

Finally, I've considered whether, on being alerted to the scam, Revolut did enough to recover Miss N's losses. As Miss N's payments were all card payments her only route of recovery would have been via a chargeback claim, and I can't see that it would have had any chance of success. The recipients of Miss N's payments were genuine crypto providers and would only need to show that they provided a service (that of providing crypto) in order to successfully defend the chargeback. That seems very likely to be the case, so I think Revolut acted fairly in not taking her chargeback claim any further.

My final decision

For the reasons I've explained, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss N to accept or reject my decision before 17 April 2024.

Lisa De Noronha
Ombudsman