DRN-5064807

The complaint

Ms M complains that Revolut Ltd didn't do enough to protect her when she fell victim to a cryptocurrency investment scam.

What happened

In early 2023, Ms M was looking for an investment opportunity online and found an opportunity to invest in cryptocurrency. She dealt with firm 'B', who turned out to be scammers, over the phone, by messages and via email. Over a period of five months Ms M understood she'd invested in cryptocurrency and paid out funds to release the profits she'd made. The scammer used AnyDesk as part of the scam. Ms M realised she'd been scammed after more and more money was requested in order to release her profits.

Ms M complained to Revolut, as she'd created an account with them to pay for the cryptocurrency. Revolut didn't uphold Ms M's complaint and said it needed more information from her. Ms M came to our service, but our Investigator ultimately concluded that Revolut wouldn't have been able to prevent her losses. Ms M disagreed and asked for an Ombudsman to reconsider her case.

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.

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 (in this case the 2017 regulations) 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 February 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.

I'm satisfied that Revolut ought to have recognised that the second card payment made to this scam carried a heightened risk of financial harm from fraud. It was for £11,400 and identifiably going to a cryptocurrency merchant. While I acknowledge Ms M declared the account purpose as cryptocurrency, I consider such a large payment on a new and rarely used account in March 2023, to a merchant where there is a known increased scam risk, ought still to have concerned Revolut that she could be at risk of financial harm.

Considering the value and account usage, I think that a proportionate response to that risk would have been for Revolut to have contacted Ms M by in-app chat to ask about the payment and why she was making it. But, had it done so, I'm not persuaded that would have prevented consumer's loss. I'll explain why.

We're aware Ms M was being guided by the scammer and had a great deal of trust in them. She's explained that she allowed them access to two of her devices via AnyDesk and she says they used this to view and make payments from her account with Revolut and also her bank account. She allowed them to see the balances of her accounts and agreed to take out borrowing on their instruction, not divulging the true reason for the funds. While the evidence we hold doesn't support them scammer acting on Ms M's behalf in Revolut account – which I will address later – this overall testimony reinforces the trust Ms M had in the scammer.

Ms M, via her representative, has provided some mixed information about whether it was her who selected the reasons disclosed for borrowing/sending the funds used in this case. For example at one stage she explained the scammers took charge of the transactions in her banking, when a payment reason of "Something else" was selected. Then at another time it's been explained she selected this reason because she didn't understand cryptocurrency or investing. While this happened on Ms M's bank account, not Revolut, I think it's important for considering Ms M's mindset at the time of the scam.

We're aware Ms M was looking for an investment opportunity herself when she found the scam. And she's told us she received training and support from the scammers around this kind of investing. I'm not persuaded by her representative's argument that this option was selected as she was *so unclear* about what was happening. I'm persuaded this option was most likely selected by Ms M on the instruction of the scammer, as Ms M had confidence in following what the scammer told her. And this was before I consider Revolut ought to have intervened.

As above, Ms M has said the scammer carried out the transactions for her as she didn't understand what was going on or how cryptocurrency worked. But Revolut has shown us that Ms M was logging in using her mobile banking app on her registered iPhone during the course of this scam. And that the transfers made as part of the scam were also done on her mobile – not on her laptop as she has suggested. As our Investigator evidenced, AnyDesk can't be used by a third party to make transfers for someone else on their iPhone. So these payments must've been done by Ms M herself, not by the scammer. I accept Ms M was very likely being coached on exactly how to do this, but the evidence indicates it must've been her taking the necessary steps.

This is all key, because it indicates that Ms M was being actively coached in the moment to make the payments for this scam. Taking Ms M's testimony at face value, she didn't fully understand the investment opportunity, but therefore defaulted to the scammer to support and guide her. Had Revolut therefore spoken to her, I'm confident she'd have sought their help again. It seems likely that the scammer was already speaking to Ms M at the time of the payments, so they'd have been on-hand to coach her through what Revolut asked. And considering the trust she had in them, as she was already allowing them access to her

devices and accounts by the time I consider Revolut should've intervened, I consider she'd have been persuaded to give the answers they instructed.

I have considered whether Revolut could've recovered any of the funds Ms M lost as a result of this scam, but I'm agreement with Revolut that a chargeback claim wouldn't have succeeded. And the transfers were for peer-to-peer purchasing of cryptocurrency. We know Ms M received the cryptocurrency in exchange for these payments, so Revolut couldn't recover these funds either.

Whilst Ms M has undoubtedly been the victim of a cruel scam, I can only uphold her complaint if I'm satisfied Revolut's failings made a material difference to what happened. For the reasons given, I'm not persuaded they would have.

My final decision

For the reasons set out above, I don't uphold Ms M's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms M to accept or reject my decision before 7 February 2025.

Amy Osborne
Ombudsman