DRN-4927994

The complaint

Mrs A complains that Revolut Ltd ('Revolut') hasn't refunded the money she lost after she fell victim to a scam.

What happened

The circumstances of the complaint are well known to both parties, so I don't intend to set these out in detail here. However, I'll provide a brief summary of what's happened.

In May 2023, Mrs A fell victim to a cryptocurrency recovery scam, whereby she thought a third party ('the scammer') was helping her to access cryptocurrency, that she believed she had purchased several years earlier, which was being held in a dormant account. As part of the scam, Mrs A opened an account with Revolut, from which she made the following debit card payments:

- £594 on 19 May 2023 to a cryptocurrency exchange platform – which I'll refer to as 'N';
- £12 on 24 May 2023 to a cryptocurrency exchange platform – which I'll refer to as 'L'; and
- £2,500 on 25 May 2023 to a cryptocurrency exchange platform – which I'll refer to as 'B'.

All the payments went to Mrs A's digital wallets with the cryptocurrency exchange platforms, which she had opened with the assistance of the scammer. The £12 payment was rejected by L and it transferred £11.42 back to Mrs A's Revolut account. However, the funds that were sent to N and B were used to purchase cryptocurrency, which was subsequently sent to the scammer. In total, Mrs A has lost £3,094.58.

In December 2023, Mrs A reported the scam to Revolut in the form of a complaint. Revolut considered raising chargebacks for the scam payments, but decided they had no reasonable prospect of success and so didn't take this further. Revolut also declined to reimburse Mrs A.

Unhappy with Revolut's response, Mrs A referred her complaint to this service. Our Investigator didn't uphold the complaint. They didn't think the first two scam payments ought to have given Revolut cause for concern and so it couldn't reasonably have been expected to have prevented those payments being made.

Our Investigator did think Revolut should've provided Mrs A with a written warning about scams involving cryptocurrency when the third scam payment was made. However, they weren't of the opinion that a written warning would've prevented Mrs A from going ahead with that payment.

Mrs A didn't agree. She thought the payments were suspicious and Revolut should've done more – through human intervention – to question her about the activity. Mrs A thought that this would've resulted in the scam being identified and the loss being prevented.

As an agreement couldn't be reached, the complaint 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.

In deciding what's fair and reasonable, I'm required to take into account relevant law and regulations, regulators' rules, guidance and standards, codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

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.

Here, it's not in dispute that Mrs A made the scam payments from her Revolut account. So, the payments were authorised and under the Payment Services Regulations, the starting position here is that Mrs A is responsible for the payments (and the subsequent loss) despite the payments being made as a result of a scam.

However, that isn't the end of the story. Good industry practice required Revolut to be on the lookout for account activity or payments that were unusual or out of character to the extent that they might indicate a fraud risk. On spotting such a payment, I'd expect it to take steps to warn the customer about the risks of proceeding.

Revolut has argued that Mrs A opened her account for the purpose of making the scam payments. As a result, Revolut didn't have any previous transactions to compare the scam payments to. However, Revolut did have some information available to it, which would've allowed it to assess the risks involved in the transactions Mrs A was making. So, I'm not persuaded Revolut couldn't have identified that Mrs A was falling victim to a scam because the account was brand-new.

When the successful scam payments were made, Revolut ought to have known that the destination of the payments were cryptocurrency exchange platforms. At the time of the payments, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency had reached record levels in 2022. By May 2023 (when Mrs A made the scam payments), Revolut ought fairly and reasonably to have recognised that there was an increased risk of fraud when its customers were using its services to purchase cryptocurrency.

So, in some circumstances, a payment to a cryptocurrency exchange platform should have caused Revolut to consider the payment as carrying an increased risk of fraud, despite the payment going to the customer's own digital wallet.

Prior to the first successful scam payment, Mrs A made three payment attempts to another cryptocurrency exchange platform – which I'll refer to as 'M'. Those payment attempts were all made within a five-minute period, but were rejected by M. As a result, Mrs A went on to make a £594 payment to N around 13 minutes later.

Whilst I appreciate the payment to N went to a cryptocurrency exchange platform, I don't consider that the payment was so remarkable that it demonstrated a risk of financial harm that ought to have given Revolut cause for concern. As a result, I don't think Revolut needed to take any steps to warn Mrs A about the risks of proceeding with the payment.

The second scam payment also went to a cryptocurrency exchange platform – this time to L. Although this was the third cryptocurrency exchange platform Mrs A had paid or attempted to pay, the value was £12 and there had been a period of five days since Mrs A previous payment to a cryptocurrency exchange platform. So, I'm not persuaded that this payment demonstrated that Mrs A was at risk of financial harm. In those circumstances, I wouldn't have reasonably expected Revolut to have done anything before processing the payment and so I don't think it could've prevented that payment being made.

The following day, Mrs A made the third scam payment, which was a £2,500 payment to B – a cryptocurrency exchange platform. This wasn't the first time Mrs A had used her Revolut account to pay a cryptocurrency exchange platform. So, a cryptocurrency purchase wasn't entirely out of character for Mrs A. However, despite the payment going to a digital wallet in Mrs A's own name, I don't think that was sufficient for Revolut to believe there wasn't a risk of fraud here. So, I've thought about whether the payment identified a heightened risk of fraud that merited its intervention.

Having opened the Revolut account, Mrs A had been topping up her account and immediately attempting to send the funds to cryptocurrency exchange platforms. Each time a payment was rejected by a merchant, Mrs A quickly changed to a different cryptocurrency exchange platform to ensure the funds were leaving her Revolut account.

The third scam payment went to a new beneficiary which was identifiably a cryptocurrency exchange platform. The value, of £2,500, was significantly larger than Mrs A's previous payments – and almost five times larger than the next largest payment on the account. This was also the fourth cryptocurrency exchange platform Mrs A had attempted to pay since opening the account a week earlier. Just minutes before making the payment to B, Mrs A had tried to send funds to N, but that payment was rejected by the merchant, resulting in Mrs A quickly moving the funds to a different beneficiary.

In those circumstances, I think Revolut should have considered that Mrs A was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I'm satisfied that Revolut should've done more to protect Mrs A from fraud.

I appreciate that Mrs A thinks Revolut ought to have questioned the scam payments through human intervention. However, I'm not persuaded the circumstances demonstrated a risk to Revolut that required human intervention. Instead, I think a proportionate response to the third scam payment would've been a tailored written warning, addressing the common hallmarks of investment scams involving cryptocurrency payments.

I can't say for certain what Mrs A would've done if she'd been provided with a tailored written warning about cryptocurrency investment scams – and that's because Revolut didn't show her one. It's possible that a written warning would've given Mrs A enough doubt about what she was being asked to do that she wouldn't have gone ahead with the payment. It's also possible that a warning wouldn't have prevented the payment being made. When I can't say for certain what would've happened, I must consider whether the available evidence shows that it was more likely than not that Mrs A would've acted differently.

Mrs A says that the scammer was professional and immediately built a relationship of trust with her. They provided Mrs A with a plausible reason for contacting her (giving her access to cryptocurrency held in a dormant account) and claimed to be representing a genuine cryptocurrency exchange platform, which Mrs A researched and found positive reviews of. The correspondence Mrs A received looked very professional, and she had no reason to believe it wasn't being sent to her from the real company.

By her own admission, Mrs A had full confidence that the scammer was legitimate and that they were looking out for her best interests. As a result, she was persuaded to give the scammer remote access to her devices and willingly followed the scammer's instructions on how to open various accounts on different platforms, which included advice on how to update her mobile phone software to allow her to download the Revolut mobile banking app. Furthermore, she felt so confident that the scammer was genuine, that she provided them with a copy of her passport.

At the time Mrs A was making the third scam payment, she had been heavily coached by the scammer over the period of a week and had been given no reason to doubt what she was being asked to do. I'm also mindful that Mrs A wasn't falling victim to a typical cryptocurrency investment scam. So, even if Revolut had provided information about the hallmarks of investment scams involving cryptocurrency, I'm not persuaded a tailored written warning would've resonated with Mrs A at the time or prevented her from going ahead with the payment.

As a result, whilst I don't think Revolut did enough to protect Mrs A from fraud when the third scam payment was made, I don't think a proportionate response to the apparent risk would've stopped the payment being made and therefore Revolut can't fairly be held responsible for the loss or be required to refund the payment.

Once it was aware of the scam, Revolut did consider attempting a chargeback with the merchants. However, Revolut decided against pursuing claims against the merchants Mrs A paid.

Here, I'm mindful the card payments went to genuine merchants – who would have arguably provided their services – so I'm not persuaded a chargeback would've had any reasonable prospect of success and would most likely have been defended by the merchants.

So, I don't find Revolut acted unfairly in not raising chargebacks as they had little prospect of success. And I don't find Revolut could've reasonably done anything further to recover Mrs A's loss.

My final decision

For the reasons explained above, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs A to accept or reject my decision before 14 May 2025.

Liam Davies
Ombudsman