DRN-5190708

The complaint

Miss R complains that Revolut Ltd didn't do enough to protect her from the financial harm caused by an investment scam, or to help her recover the money once she'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

In December 2022, Miss R was referred by a friend to someone I'll refer to as "the scammer" who said he'd help her to invest in cryptocurrency. The scammer told Miss R he worked for an investment company and that she would be making investments into stocks and shares in large companies.

The scammer communicated with Miss R via WhatsApp and told her to buy a new laptop and to download AnyDesk remote access software so he could help her with her investments. He also told her to open accounts with Revolut, "W", and a cryptocurrency exchange company, which I'll refer to as "C". The scammer asked her to first purchase cryptocurrency through C and the load it onto an online wallet. Between 14 December 2022 and 17 February 2023, she made sixteen faster payments from Bank H totalling £88,020.19. Between 21 December 2022 and 30 January 2023, she made five faster payments from W totalling £49,555.19. And between 27 January 2023 and 24 February 2023, she made eight faster payments from Bank C totalling £68,990. All these payments were to bank accounts in Miss R's own name. Then, between 24 February 2023 and 6 June 2023, she made seven payments from Revolut to a cryptocurrency account in her name totalling £43,030, (of which £1,500 was returned to the account).

When she'd used up her savings, the scammer told Miss R to take out loans to fund the investments, and in February 2023 she was passed to a more senior broker to discuss larger investments. She realised she'd been scammed when she didn't receive any returns on her investments, and she lost contact with the scammer.

She complained to Revolut arguing that it should have intervened because she was making unusual payments from a new account in a short space of time. She said she made large payments into the account on 23 February 2023, followed by payments out on 24 February 2023, which ought to have raised suspicions.

Revolut refused to refund any of the money, but Miss R wasn't satisfied and so she complained to this service. She said Revolut didn't contact her before processing the payments and it made no effort to try to help her once she reported the fraud. She said she was threatened and coerced by the scammers to take out the loans, they told her what to say to the bank, and they opened the Revolut and cryptocurrency accounts using AnyDesk.

Responding to the complaint, Revolut said Miss R was shown a new beneficiary warning as follows: *"Do you know and trust this payee? If you're unsure, don't pay them, as we may not*

be able to help you get your money back. Remember, fraudsters can impersonate others, and we will never ask you to make a payment."

It said the second payment, which was for £37,990 on 24 February 2023, was held and Miss R was asked by an agent to select a payment purpose. She selected' paying for goods and services' and was then given the following warning: *'be aware that scammers are using increasingly sophisticated techniques to gather personal information and convince customers to transfer funds in complex scams. They can pretend to be a financial institution, government institutions, trusted online merchants, an exciting investment opportunity or even people you know. They may even contact you by phone or SMS from a number that appears to belong to a trusted source, such as Revolut or another bank…Please be aware that scammers will typically offer a price below market value to attract your attention. Social media has also become an easy way for scammers to advertise their goods and services. Please do your research on the seller and try to verify if they are a genuine seller. You should check if the seller has reviews from previous customers before proceeding. If you have any concerns, then do not proceed with the purchase'*.

Our investigator didn't think the complaint should be upheld. He noted that when Miss R made the transfer on 24 February 2023, she selected 'payment for goods and services', which led to a tailored warning about goods and services scams, rather than cryptocurrency investment scams. He commented that as she was paying a cryptocurrency merchant, she should have been asked some probing questions about why she said she was paying for goods and services, and a warning about cryptocurrency investments would have been more appropriate. But he didn't think this would have stopped the scam, noting that Miss R had confirmed the scammer had guided her through each transfer and coached her on how to respond to questions from her banks.

He also commented that Miss R was asked questions by Bank H about transfers she was making from that account between 14 December 2022 and 15 December 2022. For the first three transfers, she selected 'purchase' for the payment purpose. And during a call on 14 December 2022, she said the payment was for property renovation work, she'd been given the payee details by the person doing work so they could buy building materials, and she'd met them in person. On 15 December 2022, she had a further call with Bank H when she confirmed that there was no third-party involvement and that she was moving funds to an account in her own name to top up the account.

Our investigator further noted that on 13 January 2023, Miss R attempted to make a transfer from Bank N to another account in her name. Bank N blocked the payment and questioned Miss R, when again she said the funds were intended for home improvements. Bank N asked for evidence of this and warned her she'd likely fallen victim to a scam. It then invoked the banking protocol, and eventually closed the account.

Our investigator also listened to recordings of calls Miss R had with Bank C on 23 February 2023, 24 February 2023, and 27 February 2023. During the calls, Bank C asked about the purpose of the payments and gave basic scam warnings. Miss R said she was moving money either to save it or because she wanted to spread her funds across her various accounts.

Our investigator felt that Miss R's interactions with her other banks demonstrated her determination to send the funds despite having been presented with warnings, so even if Revolut had asked more probing questions, it wouldn't have stopped the scam.
Finally, he said there wasn't a realistic prospect of a successful recovery because the payments were made to an account in Miss R's name and moved on from there.

Miss R has asked for her complaint to be reviewed by an Ombudsman.

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.

Having done so, I've reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Miss R has been the victim of a cruel scam. I know she feels strongly about this complaint, and this will come as a disappointment to her, so I'll explain why.

I'm satisfied Miss R 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although she didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of her bank account, Miss R is presumed liable for the loss in the first instance.

There's no dispute that this was a scam and even though there have been some inconsistencies in Miss R's account of what happened, on balance, I accept she was scammed. But although she didn't intend her money to go to scammers, she did authorise the disputed payments. Revolut is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

Revolut was an emoney/money remittance provider and at the time these events took place it wasn't subject to all of the same rules, regulations and best practice that applied to banks and building societies. But it was subject to the FCA's Principles for Businesses and BCOBS 2 and owed a duty of care to protect its customers against the risk of fraud and scams so far as reasonably possible.

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 September 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;

• have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;

• 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've thought about whether Revolut could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to a genuine cryptocurrency exchange company. However, Revolut ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it did enough to warn Miss R when she tried to make the payments.

Miss R was shown a new payee warning on 24 February 2023 when she made the first payment to C, and when she made a payment of £37,990 a few minutes later, Revolut contacted her via its live-chat facility and asked for a payment purpose. Miss R said she was paying for goods and services and was shown a warning relevant to that response. I've considered whether this was proportionate to the risk presented by the payment and while I accept Revolut was prevented from identifying that she'd been scammed because of the response she gave, Miss R was paying £37,990 to a cryptocurrency merchant, which wasn't consistent with the payment purpose she gave. Because of this, it should have asked her some probing questions about the purpose of the payment and given her a warning tailored to cryptocurrency scams.

However, even if Revolut had asked more probing questions, I don't think it would have detected the scam. This is because Miss R has explained that she'd been coached to lie and so I'm satisfied the scammer would have guided her to provide more satisfactory responses to Revolut's questions. There's also evidence from her interactions with her other banks that she had no intention of disclosing the real purpose of the payments, so I don't think she'd have answered truthfully if she'd been asked more probing questions.

I've also considered whether a tailored warning about cryptocurrency investment scams would have made any difference and I don't think it would have. Miss R ignored the new payee warning and the purchase scam warning from Revolut, she was happy to lie to her banks to ensure the transfers were processed and to fund the investment with money from loans, and she's told us she checked the FCA website at the start, so she was confident the investment was genuine. S, I don't think a written warning so early in in the scam period would have prevented her loss.

Miss R disputes that it's fair to reach a conclusion based on how she might have reacted to a better intervention, but I have carefully considered all the evidence and reached a conclusion on what I think is likely to have happened if Revolut had done what we'd expect it to have done, and I'm satisfied that's fair.

Recovery

I don't think there was a realistic prospect of a successful recovery because Miss R paid an account in her own name and moved the funds onwards from there.

Compensation

The main cause for the upset was the scammer who persuaded Miss R to part with her funds. I haven't found any errors or delays to Revolut's investigation, so I don't think she is entitled to any compensation.

I'm sorry to hear Miss R has lost money and the effect this has had on her. But for the reasons I've explained, I don't think Revolut is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

My final decision

For the reasons I've outlined 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 Miss R to accept or reject my decision before 14 January 2025.

Carolyn Bonnell
Ombudsman