DRN-5013666

The complaint

Mrs F complains that Revolut Ltd didn't do enough to protect her from the financial harm caused by an advance fee 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 May 2023, Mrs F received a text message from an unknown number about an opportunity to work as a 'data generator' for a company I'll refer to as "M". She didn't think this was suspicious because she'd been looking for work and had submitted multiple applications to online recruitment agencies. She searched for the number on a social media site and concluded it was genuine and subsequently spoke to someone posing as a recruiter, who I'll refer to as "the scammer".

The scammer seemed very professional and explained she'd be required to review different products online to boost company sales, in return for a commission on each task. The scammer explained she would need to pay for tasks in cryptocurrency and that the basic commission for five days work would be 500 USDT.

The scammer asked her to first purchase cryptocurrency and then load it onto an online wallet. Between 10 May 2023 and 24 May 2023, Mrs F made eight faster payments, two card payments, and two push-to-card payments to five different beneficiaries totalling £78,470.17. She realised she'd been scammed when she tried to withdraw her commission and was told she'd have to pay further fees and tax.

Mrs F complained to Revolut, but it refused to refund any of the money she'd lost, explaining the chargeback claims were invalid because the card payments had been authenticated through 3DS and there was no fraudulent activity on the account.

Mrs F wasn't satisfied and so she complained to this service with the assistance of a representative who argued that Revolut should have intervened because she was making multiple payments to new payees in quick succession from a newly opened account immediately after receiving high value credits into the account. They said it should have asked her whether there were any third parties involved, how she met them, and whether the rate of return was plausible, and as she believed the job was genuine and she hadn't been coached to lie, Revolut would have uncovered the scam.
Responding to the complaint, Revolut said Mrs F created the account on 8 May 2023, giving multiple account purposes. It said the account was newly created and so there was no transaction history to compare the payments with, and that its controls were proportionate and appropriate.

It explained that Mrs F was shown a new payee warning each time she added a new beneficiary and that its fraud system was triggered several times. When she made payments for £3,600, £6,800, and £1,500, she selected 'Transfer to a Safe Account' and shown strong

warnings according to the stated purpose before she proceeded with the payments. Further interventions occurred when she made payments for £10,000, £11,564, £11,000, and £12,000. She was required to engage in a 'payment purpose review' conversation via live chat where she said she was transferring funds to a safe account, she wasn't being pressured to make the transactions, she hadn't been asked to disregard warnings, and she hadn't downloaded remote access software.

Revolut also said Mrs F failed to research M, she went ahead with the payments despite strong warnings in the app and on the chat, she was making payments in cryptocurrency for something she was expecting to be paid for and for which the returns were too good to be true, and she lied when providing a payment purpose which prevented it from detecting the scam. In addition, it argued that the activity isn't a normal or legitimate type of employment and may be considered a scam itself.

It said that it attempted to recover the funds by contacting the beneficiary institutions on 30 September 2023, but it didn't receive a response. It's not possible to recover push-to-card payments and the chargeback requests were rejected because there was no fraudulent activity on the account as the transactions were authenticated through 3DS.

Revolut argued that the card payments were self-to-self payments and for this service to effectively apply the reimbursement rules to self-to-self transactions is an error of law. It also cited the Supreme Court's judgement in Philipp v Barclays Bank UK plc [2023] UKSC 25 where Court held that in the context of APP fraud, where the validity of the instruction is not in doubt, "no inquiries are needed to clarify or verify what the bank must do. The bank's duty is to execute the instruction and any refusal or failure to do so will prima facie be a breach of duty by the bank."

Our investigator didn't think the complaint should be upheld. He explained that the first in app intervention, occurred on 16 May 2023. Mrs F selected 'transfer to a safe account' as the payment purpose and Revolut displayed a warning about 'safe account' scams before seeking to clarify the reason for the payment via the in-app chat. Mrs F said she was moving money to a 'trusted account' and hadn't been contacted by someone asking her to move money. Revolut blocked another payment on 19 May 2023, and after choosing safe account for the purpose of payment, she was asked the same questions regarding safe account scams and provided the same answers.

Our investigator commented that there was no evidence that Mrs F had been coached to lie, but her responses had prevented Revolut from detecting the scam. He was also satisfied that Mrs F's messages to the scammer showed she trusted the scammer and believed the job was genuine. So, there was nothing further it could have done on the occasions it did intervene.

He further commented that Revolut could have done more on 21 May 2023 because Mrs F was sending funds to a cryptocurrency merchant. He explained that a proportionate response would have been for Revolut to have shown a written warning which was tailored to cryptocurrency investment scams. But he didn't think this would have made any difference because she'd gone ahead with the previous payments having received scam warnings in the app and her responses to Revolut's enquiries showed she was determined to make the payments to the extent that she wasn't open about the purpose of the payments. So, he didn't think a written warning would have changed her mind.

Finally, our investigator said he was satisfied that Revolut did what it could to recover Mrs F's bank transfers once it was aware of the fraud but no funds remained, and it wouldn't have been able to recover the push-to-card payments because fraudsters will seek to utilise victim's funds as quickly as possible and two weeks had passed before Mrs F reported the

fraud to Revolut. Regarding the card payments, he explained that Mrs F paid a legitimate cryptocurrency exchange, and would have received a service, so there was no reasonable prospect of a successful chargeback. And he didn't think she was entitled to any compensation.

Mrs F has asked for her complaint to be reviewed by an Ombudsman. Her representative has argued that there is no evidence to support that further intervention, or tailored warnings wouldn't have stopped the scam and that there is no situation where 'safe account' would be a legitimate payment purpose. They disagree that Revolut sought to clarify why Mrs F selected 'safe account' and instead showed a safe scam warning and asked if it related to her situation, to which she responded, "no it's not, I am moving my money to a trusted safe place". They believe Revolut ought to have asked more probing and open-ended questions which would have stopped the scam.

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 Mrs F 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 Mrs F '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, she is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mrs F 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

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 May 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;

• 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. It 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 ought to have intervened to warn Mrs F when she tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Revolut to intervene with a view to protecting her from financial harm due to fraud.

Revolut intervened several times during the scam period, so I've considered whether the interventions were appropriate and proportionate to the risk presented by the payments.

The first payment was a low value payment to an account with no apparent links to cryptocurrency, and so Revolut didn't need to intervene. When Mrs F made the second payment, Revolut asked her to provide a payment purpose and then provided a warning relevant to safe account scams. I'm satisfied that Mrs F's response prevented it from detecting the scam and as this was a transfer of £3,600 to a merchant with no obvious links to cryptocurrency, I'm satisfied the intervention was proportionate to the risk presented by the payment. The next two interventions followed the same format, and again, I'm satisfied this was proportionate, and that Mrs F's response prevented Revolt from detecting the scam.

Revolut intervened a further four times. Each time, Mrs F was asked to provide a payment purpose and directed to engage in a live chat with one of its agents where she was shown a strong warning about safe account scams. She confirmed this wasn't relevant to her situation and she was sending funds to a 'trusted safe place'. She was also asked whether she'd been told she'd been a victim of fraud and rushed into making the payment, whether she'd been asked to ignore scam warnings, and whether she'd been asked to download remote access software. Mrs F responded negatively to these questions before the payments were processed.

I've considered whether Revolut did enough here, and I'm satisfied that it showed Mrs F a warning which was relevant to the payment purpose she gave, and that Mrs F's response prevented it from detecting the scam. I'm also satisfied that it took further steps to check she wasn't falling victim to a safe account scam and that it was reasonable to have taken her responses at face value. I'm also satisfied that it wouldn't have been appropriate to show Mrs F a warning tailored to cryptocurrency investment scams because there was nothing to suggest that this might be relevant.

Our investigator felt that Revolut should have intervened when Mrs F transferred funds to a cryptocurrency exchange company, particularly on 23 May 2023 when she made a card payment of £8,900 to M, and I agree with this because it was a large payment to a cryptocurrency merchant. Based on the value of the payment, I think a proportionate response would have been for Revolut to have shown a written warning tailored to cryptocurrency scams covering some of the key features of cryptocurrency-related investment scams, for example:

• Victims are usually targeted via social media or email.

• Scammers will utilise fake positive reviews from other individuals, or fake celebrity endorsements, to persuade you the investment opportunity is legitimate.

• Fake online trading platforms can appear professional and legitimate.

• Genuine investment firms won't require you to pay money in order to withdraw your returns.

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case, and, on balance, I don't think it would have. This is primarily because Mrs F didn't consider she was investing in cryptocurrency, instead she was buying cryptocurrency to pay for tasks which she expected to be paid for. So, I don't think the warning would have resonated with her. Further, even though there's no evidence Mrs F was coached to lie, the available evidence shows she believed the job was genuine and that she was determined to make the payments to the extent that the misled Revolut about the purpose of the payments.

Therefore, on balance, had Revolut provided Mrs F with an impactful warning that gave details about cryptocurrency investment scams and how she could protect herself from the risk of fraud, I don't think it would have made her pause and look more closely at what she was being asked to do. So, while I think it did miss an opportunity to intervene, I don't think this represented a missed opportunity to have prevented Mrs F's loss.

I'm sorry to hear Mrs F 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.

Recovery

Too much time had passed by the time Mrs F reported the scam to Revolut and so I don't think there was a realistic prospect of a successful recovery of the transfers. And it wasn't possible to recovery the push-to-card payments.

I've thought about whether Revolut could have done more to recover the card payments when Mrs F reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Revolut) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mrs F).

Mrs F's own testimony supports that she used cryptocurrency exchanges to facilitate the card payments. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchange would have been able to evidence they'd done what was asked of them. That is, in exchange for Mrs F's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Revolut's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

Compensation

The main cause for the upset was the scammer who persuaded Mrs F 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.

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 Mrs F to accept or reject my decision before 30 June 2025.

Carolyn Bonnell
Ombudsman