DRN-5016603

The complaint

Ms Z complains that Revolut Ltd ('Revolut') won't refund the money she lost when she fell victim to a scam.

What happened

Ms Z says that in March 2023 she met a man on a dating site who said that he could help her to earn money by investing in cryptocurrency. She says that initially she didn't believe him but after he gave her some cryptocurrency, she felt he was genuine. The person Ms Z met taught her how to invest. Initially she was advised to download a cryptocurrency app and buy cryptocurrency from various sellers via the peer to peer method. The cryptocurrency was then transferred to a platform. Ms Z says it looked like she'd made a lot of money but when she wanted to withdraw her profit the fraudster asked her to make a significant payment and then disappeared. At this point she realised she was the victim of a scam.

I have set out in the table below the transfers Miss Z made from her Revolut account.

Transaction	Date	Method	Recipient	Amount
1	10/04/23	Transfer	Company 1	£1,000
2	11/04/23	Transfer	Individual 1	£1,000
3	27/04/23	Transfer	Company 1	£1,900
4	29/04/23	Transfer	Individual 2	£1,900
5	29/04/23	Transfer	Company 1	£1,900
6	29/04/23	Push to card transfer	Individual 3	£1,800
7	30/04/23	Push to card transfer	Individual 3	£100
8	30/04/23	Transfer	Individual 4	£500
9	30/04/23	Transfer	Company 1	£2,800
10	30/04/23	Transfer	Individual 4	£700
11	04/05/23	Push to card transfer	Individual 5	£1,100
12	04/05/23	Push to card transfer	Individual 5	£1,900
Total				**£16,600**

Ms Z reported what had happened to Revolut on 14 May 2023.

Revolut didn't agree to reimburse Ms Z's loss. It said it wasn't at fault for processing the payments and that it provided warnings when each new payee was created. In addition to this, Revolut said it recognised some of the transactions were suspicious and provided educational story screens based on the scam risk. Revolut noted it had tried to recover Ms Z's funds, but no funds remained to be returned.

Ms Z was unhappy with Revolut's response and brought a complaint to this service. She said Revolut didn't protect her or recover her funds and it was irresponsible of it to close her account.

Our investigation so far

The investigator who considered this complaint didn't recommend that it be upheld. He said Revolut should have identified that payments were unusual or suspicious and contacted Ms Z before processing them. But the investigator didn't think intervention by Revolut would have made a difference. This was because it was clear from Ms Z's chats with the scammer that she had built up a strong relationship and that she didn't plan to tell the truth about the payment reason. The investigator referred to intervention by other banks Ms Z also used to make scam payments and to the fact one bank invoked the Banking Protocol. Overall, he felt Ms Z wouldn't have told the truth and that even if Revolut stopped any of the payments, Ms Z would have found another way to make it. Finally, the investigator said Revolut's terms and conditions allow it to close an account without giving a reason.

Ms Z didn't agree with the investigator's findings and asked that an ombudsman review her complaint. In summary, she said:

- Revolut didn't adhere to the Quincecare Duty. It should have stopped her payments and seriously considered whether her answers were suspicious.
- She doesn't agree that if Revolut had taken appropriate steps the scam would not have been uncovered. Another bank stopped a payment on 11 May 2023 even though she told it the payment was to buy a product. Since then, she hasn't made any further payments from any of her accounts.
- She was exploited by a scammer at a time when she was vulnerable. Her husband passed away at the end of October 2022 after a sudden illness. Ms Z has explained that at the time of the scam she was struggling with grief, loneliness, severe anxiety, and depression. In addition to this, her only daughter disappeared from her life in December 2022 and took property from Ms Z. The combination of these factors had a severe impact on Ms Z's physical and mental health and led to her being taken advantage of.

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 am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and 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 Electronic Money Institutions (EMIs) like Revolut are 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.

The Lending Standards Board's Contingent Reimbursement Model Code (CRM Code) doesn't apply in this case so I can't apply its provisions, including those that relate to vulnerability. Revolut hasn't signed up to the CRM Code but even if it had there are other reasons why Ms Z's complaint couldn't be considered under it, which I don't need to go into here. So, although I recognise Ms Z was vulnerable to this scam, I can't see that she communicated this to Revolut – meaning that Revolut had no reason to provide any additional support.

But I consider that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

I consider it fair and reasonable that at the time Ms Z made the payments 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); and
- 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.

In this case, I'm mindful Ms Z didn't have an existing relationship with Revolut as the account was opened on 10 April 2023 for the purpose of completing the scam transactions. This means that Revolut didn't understand Ms Z's normal spending patterns. When Ms Z opened her Revolut account she chose multiple reasons for opening it, including transfers and cryptocurrency.

Each time Ms Z created a new payee (so payments 1, 2, 4, 6, 8 and 11) Revolut provided a new payee warning that said:

"*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."

In addition to this, Revolut provided further warnings in respect of payments 1, 2, 3, 4 and 10. Ms Z was shown a screen that said:

This transfer may be a scam

Our systems identified this transfer highly unusual and put it on hold

Your transfer is more unusual than

99.2%

of all Revolut transfers

Revolut then provided educational storyboard messages about victims of scams losing millions of pounds a year and fraudsters being professionals. Ms Z was then presented with another screen and was asked to provide the purpose of each of the payments, following which she was provided with a warning tailored to the payment reason chosen.

Due to a technical glitch Revolut hasn't been able to provide the reasons Ms Z provided for each of the transactions. But the messages Ms Z exchanged with the scammer, which I will discuss below, lead me to believe it's more likely than not that she didn't say she was buying cryptocurrency.

Finally, in respect of the push to card payments in the table above, Revolut provided a further warning which advised Ms Z should never pay someone she doesn't know and trust.

I'm satisfied that Revolut went far enough when most of the transactions were made. For the early payments I consider that Revolut only needed to provide a warning that broadly covers scams and that it did so. As Ms Z made further payments, I'd expect Revolut to provide warnings tailored to the payment purpose Ms Z chose. I've seen evidence that tailored warnings were provided at the points I have set out above. Revolut can only provide a warning based on the payment reason chosen.

While its arguable Revolut should have asked Ms Z to answer questions in the chat, probably at around the time she made transaction ten on 30 April 2023, I'm not persuaded that doing so would have made a difference in the particular circumstances of this case.

I have asked Ms Z to provide me with all the messages she exchanged with the scammer, but she has provided very limited evidence. Ms Z says messages have been deleted by accident.

I can see that when Ms Z reported the scam to Revolut on 14 May 2023 she noted that the scammer "told me not to write any words about cryptocurrency". I've also seen a message the scammer sent to Ms Z on 3 April 2023 which advises her not to tell her bank she is buying cryptocurrency. And in a further message later that day, the scammer told Ms Z that she needed to go to her bank the next day and just say she is transferring money to a friend. The scammer went on to say that Ms Z could say anything she wanted to the bank, as long as the bank believes it. Finally, I've seen a screenshot of some information provided to Ms Z which advises not to include cryptocurrency related terms in the payment reference as the payment might be blocked by the bank.

I have also listened to calls between Ms Z and a different bank which intervened when she made payments. This is the same bank that later invoked the Banking Protocol. This bank was concerned that Ms Z was falling victim to a scam and asked her questions about certain payments and transfers. Ms Z didn't answer the questions posed honestly and didn't say she was investing. Instead, Ms Z said she was paying a friend or to buy goods.

On 11 May 2023, at around the time the Banking Protocol was invoked, Ms Z discussed with the scammer the questions she might be asked and assured him she wouldn't mention cryptocurrency. Ms Z also said she would delete the investment app 'again' when she saw the bank or the police. Ms Z clearly had a cover story prepared for when the police spoke to her.

Revolut is an EMI which communicates through its chat function in the app. So, if Revolut were to have asked Ms Z questions about the transactions, it would have done so in the app. The evidence I have seen leads me to conclude that if Revolut had asked questions about any of the payments Ms Z would not have been honest. I appreciate that this was because she was under the spell of a cruel scammer, but I can't see that the scam would have been uncovered if Revolut had asked Ms Z questions in its chat facility.

Ms Z has noted that the scam came to light on 11 May 2023 when a bank she was transferring funds from intervened and invoked the Banking Protocol. It's clear that the bank that invoked the Banking Protocol had much more information about Ms Z because she had an existing relationship with it. For example, the bank concerned knew about the death of her husband and that Ms Z had disputed a payment in the past. Revolut didn't have this information because the account was newly opened. The bank that invoked the Banking Protocol had also intervened on previous occasions and had concerns about the information Ms Z provided it with and whether she was being honest in phone calls. So, by the time it invoked the Banking Protocol, Ms Z's bank had a lot of concerning information and had spoken to her multiple times.

It's not clear if Revolut has closed Ms Z's account but if it has, I agree with the investigator that Revolut's terms and conditions allow it to close an account with notice.

Finally, I've thought about whether Revolut could have done more to recover Ms Z's funds. But, as Ms Z bought cryptocurrency from legitimate sellers, and then passed it on to the scammer, there is no prospect of recovery.

Overall, whilst I'm sorry to hear about this cruel scam, I can't reasonably ask Revolut to reimburse Ms Z.

My final decision

For the reasons stated, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms Z to accept or reject my decision before 26 December 2024.

Jay Hadfield
Ombudsman